Computing on Quantum Shared Secrets for General Quantum Access Structures

Roozbeh Bassirian[1], Sadra Boreiri[1,2], and Vahid Karimipour[2]

[1] Department of Computer Engineering, Sharif University of Technology, P.O. Box 11155-9161, Tehran, Iran.
[2] Department of Physics, Sharif University of Technology, P.O. Box 11155-9161, Tehran, Iran.

Abstract

Quantum secret sharing is a method for sharing a secret quantum state among a number of individuals such that certain authorized subsets of participants can recover the secret shared state by collaboration and other subsets cannot. In this paper, we first propose a method for sharing a quantum secret in a basic $(2, 3)$ threshold scheme, only by using qubits and the 7-qubit CSS code. Based on this $(2, 3)$ scheme, we propose a new (n, n) scheme and we also construct a quantum secret sharing scheme for any quantum access structure by induction. Secondly, based on the techniques of performing quantum computation on 7-qubit CSS codes, we introduce a method that authorized subsets can perform universal quantum computation on this shared state, without the need for recovering it. This generalizes recent attempts for doing quantum computation on (n, n) threshold schemes.

1 Introduction

Secret sharing refers to procedures for distributing a secret among a group of participants, each of whom is allocated a share of the secret such that only certain qualified subsets of participants, known as authorized parties, can collaboratively reconstruct the secret. Secret sharing was first introduced independently by Adi Shamir [1] and George Blakley[2] in 1979, where both secret and shares were classical information. Quantum Secret Sharing (QSS) is a natural extension of the classical protocol to the quantum realm [3, 4, 5] where quantum mechanics provides a way for security of sharing the classical secret. This was even further extended to the case of Quantum State Sharing, in which a quantum state $|\psi\rangle$ is distributed among a group of parties in such a way that it can be retrieved only by their collaboration [6, 7]. In addition, some scholars have worked on information theoretical models for the quantum secret sharing [8, 9].

A most interesting line of development in this subject concerns itself not only with methods of sharing and retrieving a state, but also with ways of performing universal quantum computation on such a state by the authorized parties, who may not even need to know what the state is. This is a subject in the field of distributed computation and quantum cryptography, the latter being one of the most promising fields in quantum computation. While some of the well-established protocols have been experimentally performed [10, 11, 12], and even commercialized, new ones with different domains of applications are being proposed. Blind quantum computation [13, 14], quantum homomorphic encryption [15], sharing of classical data [16, 17, 18] and quantum states [5, 6, 7, 19], proactive quantum

secret sharing [20], and even performing quantum computation on shared secrets [21] are good examples of these protocols.

To be more specific, suppose Alice wants to encode a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to $|\overline{\psi}\rangle = \alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$ and shares it among n participants such that only certain subsets can retrieve the state.

The most common and the simplest access structure, is the one denoted by (n, n) where the only authorized subset is the whole set. It generalizes to the (k, n) access structure, where any subset of size k can recover the data by collaboration [6]. In this so called threshold schemes, the simplest one is the $(2, 3)$ scheme proposed in [6], which uses qutrits (3-level states) and the following encoding:

$$|\overline{0}\rangle = \tfrac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle) \quad (1)$$

$$|\overline{1}\rangle = \tfrac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle) \quad (2)$$

$$|\overline{2}\rangle = \tfrac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle). \quad (3)$$

It is readily seen that any two members (say 1 and 2) can retrieve the state by simply performing the operator $C_{21}C_{12}$ on their qutrits, where C_{ij} is the CNOT operator which is controlled by i and acts on j in the form $C_{ij}|\alpha, \beta\rangle_{i,j} = |\alpha, \alpha + \beta\rangle_{ij}$.

There are many applications where the members do not have an equal level of authorization. The most general access structure is where only certain subsets of the set of receivers can retrieve the classical or the quantum data. An example of an access structure is when the whole set is $X = \{A, B, C, D\}$ and the authorized subsets are $\mathcal{A}(X) = \{\{A, B, C\}, \{B, C, D\}\}$. Obviously this is not a threshold scheme, since the subset $\{A, B, D\}$, although having 3 members is not an authorized subset.

While there has been a lot of progress in QSS schemes for (n, n) and (k, n) threshold structures, much less has been reported on these schemes for general access structures. In this respect we can mention [6, 7], where arbitrary quantum access structures are constructed and a relation with quantum error correcting codes has been established. We should emphasize however that these schemes use $d-$ level states for quantum state sharing, as specified in the example of equation (1) and d increases with complexity of access structure. In addition, some recent attempts to reduce the number of quantum shares to make more efficient schemes have been done [22, 23].

On the other hand, quite recently it has been shown [21] that shared and secret quantum computation is possible on an (n, n) scheme, using only qubits. For performing a specific computation, each party member applies a relevant operation on his or her corresponding share. They are also allowed to use ancilla qubits and public announcement of their measurement results. While the desired quantum circuit is known to every party member, during the computation no information leaks to the un-authorized parties, neither about the input nor the output secret state [21].

It might seem natural that performing a distributed secret computation on even a threshold access structure, let alone the general access structure, should utilize high $d-$ level states for which theoretical and experimental tools are not as developed as for qubits. The aim of our work is to fill this gap and to construct QSS schemes for general access structures using qubits, and to perform distributed quantum computation on them.

Our method is based on general ideas of [7] and [21]. We use the same induction steps proposed in [7]. However, in all the steps we use new QSS schemes based on the 7-qubit code as building blocks, and we use our purification method which makes distributed quantum computation possible for these

schemes. While in [7] it is proved that any purification method works, the steps of purification are not explicitly specified. This explicit purification is necessary if we want to do quantum computation on these shared quantum states. It is worth mentioning that using our purification method, it is also possible to do universal quantum computation on the QSS schemes proposed in [7]. However, it would require ancillary states for every gate. The advantage of using 7-qubit code is that it limits the usage of ancillary states to only the $\frac{\pi}{8}$-gate.

The structure of this paper is as follows: In Section 2, we explain our notations and conventions. In Section 3, two QSS schemes are proposed for two basic access structures which will act as building blocks of arbitrary access structures. Section 4 shows how universal computation is possible on these basic access structures and section 5 is devoted to computation on general access structures. The paper ends with a conclusion and outlook.

2 Preliminaries

We assume that the reader is familiar with basic concepts of error correcting codes[24] and stabilizer formalism[25]. In this section, we review some definitions and notations for future use.
In the context of secret sharing, an access structure identifies whether a group of parties should have access to a particular data. In set-theoretic concepts, an access structure marks every subset of a group as authorized or unauthorized. Thus, authorized subsets of an access structure are those subsets that are qualified to access the desired data. More formally, we have:

Definition 1. For a given set X of players, an **access structure** $\mathcal{A}(X)$ is a collection of authorized subsets of X, $\mathcal{A}(X) \subseteq 2^X$, where 2^X is the power set of X, with the monotone increasing property which is a natural property for authorized subsets. More precisely, if S belongs to $\mathcal{A}(X)$, every superset T of S (i.e. any set T where $S \subseteq T$) should also belong to $\mathcal{A}(X)$

Example 1. We use the notation of (k, n) for threshold schemes, which basically refers to an access structure in which there exist n players and every subset of at least k parties is authorized. For example for the $(2, 3)$ threshold scheme when the whole set is $X = \{A, B, C\}$, the authorized subsets are $\mathcal{A}(X) = \{\{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}$.

For the sake of brevity a subset like $\{A, B\}$ is denoted simply by AB. Thus the previous access structure is simply denoted by $\mathcal{A}(X) = \{AB, AC, BC, ABC\}$. To prevent cluttering of notation, in all the discussions and figures which follow, we use the same letter A both for the player and for the (classical or quantum) share he or she receives in the scheme. In cases like above that a player A receives multiple shares, they are denoted by subscripts i.e. A_1, A_2, etc.

Definition 2. For a given set X of players, a **quantum access structure** $\mathcal{A}(X)$ is an access structure on X which also satisfies an extra condition imposed by the no-cloning theorem: For every $S, T \in \mathcal{A}(X)$, $S \cap T \neq \varnothing$.

Remark. Not all the access structures are admissible in the quantum world and there cannot exist disjoint authorized subsets in a quantum access structure. If two disjoint authorized subsets exist in $\mathcal{A}(X)$ then the following procedure can be used to make two disjoint copies of an arbitrary quantum state. First, apply $\mathcal{A}(X)$ scheme to the state, then take two disjoint authorized subsets and reconstruct two copies of the state. This contradicts the no-cloning theorem, which asserts that no operation can generate multiple copies of an unknown arbitrary quantum state [26].

Hereafter, whenever we mention access structure, we mean quantum access structure.

Definition 3. In every access structure, there are a number of subsets which we call the **minimal authorized subsets**. Due to the monotone property of the access structure, every larger subset which contains one of these subsets or the union of them is automatically authorized and need not be written explicitly in the structure. The notation simplifies a lot if we denote any access structure only by its minimal authorized subsets inside a bracket. An access structure $\mathcal{A}$ is usually indicated by $\mathcal{A} = \langle T_1, T_2, \cdots, T_r \rangle$, where T_is are its minimal authorized subsets. Thus in example 1, we write $\mathcal{A}(X) = \{AB, AC, BC, ABC\} = \langle AB, AC, BC \rangle$.

Of special importance are the class of maximal access structures. Consider the set $X = \{A, B, C\}$, the $(2, 3)$ threshold scheme access structure $\mathcal{A}(X) = \{AB, AC, BC, ABC\}$, has the property that for any member of 2^X, either itself or its complement belong to $\mathcal{A}(X)$. More formally we have:

Definition 4. [7] For a given set X of players, an access structure is **maximal** and denoted by $\overline{\mathcal{A}}(X)$ if for every $S \subset X$, it satisfies:

(i) If $S \in \overline{\mathcal{A}}(X)$, then $S^c \notin \overline{\mathcal{A}}(X)$

(ii) If $S \notin \overline{\mathcal{A}}(X)$, then $S^c \in \overline{\mathcal{A}}(X)$

where $S^c = X \setminus S$.

Obviously the threshold schemes (n, n) are not maximal. As another example, for the set $X = \{A, B, C, E\}$, the structure $\overline{\mathcal{A}} = \langle AE, BE, CE, ABC \rangle$ is maximal while $\mathcal{A} = \langle AE, BE, ABC \rangle$ is not. Moreover if from a maximal access structure a member is removed, the resulting structure will no longer be maximal. [1]

Let $X = \{A_1, A_2, A_3, \cdots\}$ be a set. The aim of quantum state sharing is to encode a qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to a multi-qubit pure state $\left|\overline{\psi}\right\rangle = \alpha|\overline{0}\rangle_{\overline{X}} + \beta|\overline{1}\rangle_{\overline{X}}$ and share it to the members of X such that every authorized subset in the access structure $\mathcal{A}(X)$ can recover the original state and no unauthorized subset can retrieve it. Depending on the access structure, the number of multi-qubits may be larger than the size of X and different members of the set X may hold different numbers of qubits. This enlarged number of qubits is denoted by $\overline{X}$. The following figure is used to denote such a sharing scheme, where, by s_0 we mean a quantum state (not a classical bit).

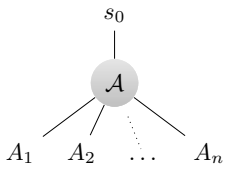

Figure 1: This symbol means that the state s_0 can be recovered by the players A_1 to A_n according to the access structure $\mathcal{A}$.

Remark. One can think of the bulb $\mathcal{A}$ both as the access structure and as the encoding circuit which encodes the state s_0 to a multi-qubit state according to that structure. When such figures are concatenated, the corresponding quantum circuits are concatenated too.

[1] More precisely, if the discarded share contains no important data, which means it is not included in any minimal authorized set, the resulting access structure is still maximal. This means that the purification produces a redundant share, that is what we desire.

Moreover, as we will show it is possible to do universal quantum computation on the same access structure. We will show that it is possible that a universal set of gates $\mathcal{P} = \{\text{CNOT}, H, S, T, X, Z\}$ be implemented on the shared state by local actions of each player on the qubit in his or her possession, eliminating the overhead for encoding and decoding of the shared state and hence preventing any leakage of the input and output shared secret to the unauthorized parties. As we will see, all the above gates are implemented in a transversal way (share-wise gates) except the T gate which requires communications between the players.

We will frequently use the threshold access structure $\mathcal{A} := (2, 3)$ in which any two players can retrieve the state which has been shared between three players. This is denoted by Fig. 2, the special figure where there is no symbol on the bulb:

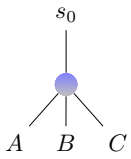

Figure 2: The symbol with no sign on it always denote the (2,3) access structure. See the caption of figure (1).

It may also happen that we have to discard some of the qubits in which case we denote the corresponding lines as dashed. The necessity of discarding some of the qubits stems from the fact that construction of non-maximal access structures can be achieved by discarding shares from secret sharing schemes with maximal access structure (Fig. 3).

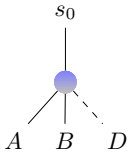

Figure 3: A dashed line means that the share of this player can be discarded. The other two players can still retrieve the state s_0 from the density matrix obtained by tracing over D.

This means that even if the pure state $|\overline{\psi}\rangle$ is traced over D, the two parties A and B are still capable of retrieving the state s_0 from the remaining mixed state ρ_{AB}. More concretely if a state $|\psi\rangle$ has been encoded to $|\overline{\psi}\rangle_{ABD}$ such that any two players, say A and B can collaborate so that the initial state is recovered by one of them say A. This means that there is a recovery operation $\mathcal{R}_{AB}$ such that

$$\mathcal{R}_{AB}(|\overline{\psi}\rangle_{ABD}\langle\overline{\psi}|) = |\psi\rangle_A\langle\psi| \otimes \chi_{BD} \tag{4}$$

Since Tr_D commutes with $\mathcal{R}_{AB}$, this means that the same kind of recovery operation by A and B will retrieve the state, that is:

$$\mathcal{R}_{AB}\left(\text{Tr}_D(|\overline{\psi}\rangle_{ABD}\langle\overline{\psi}|)\right) = |\psi\rangle_A\langle\psi| \otimes \text{Tr}_D(\chi_{BD}) \tag{5}$$

In such a case, the discarded share is represented by a dashed line. This action of discarding (tracing out) will play a major role in our construction of more complex concatenated schemes.

Finally, we concatenate simple QSS schemes (expanding a share of access structure S_1 using access structure S_2) to implement more complex access structures [7]. As an example consider Fig. 4. Depending on which of the participants in the list set $X = \{A, B, C, D, E, F\}$ will hold the share G, we can implement different access structures for the set X, i.e. if $G = A$, then the access structure contains the sets AB and AC, while if $G = B$, it will contain the sets AB and BC. In both cases, the subsets of $\{D, E, F\}$ remain unauthorized. Note that G being more than one qubit, can be shared between more than two members, i.e. it can be given to A and D, in which case the access structure will be more complex. Note that in concatenated schemes, no information can be gained from unauthorized sets of different instances of access structures [7]. For example, in Fig. (4), no information is leaked from A and D alone. Thus, while checking the authority of a given set, we have to be able to recover the secret recursively from the bottom if it is authorized, and it does not contain any information about the secret if it cannot recover the secret in this manner.

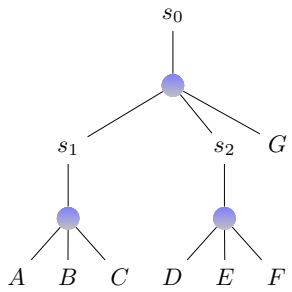

Figure 4: Concatenated access structures: Depending on whether the extra share G is given to A or to B, different access structures are obtained.

3 Quantum state sharing using 7-qubit code

The original (2,3) scheme is based on using 3-level states as in (1). We will construct all the QSS schemes from a basic threshold (2,3) scheme which is based on using the 7-qubit code. The 7-qubit code is a $[[7, 1, 3]]$ CSS code[27], which encodes one qubit into seven qubits in such a way that the distance between all the states involved is at least 3. The code is based on the classical $[7, 4, 3]$ hamming code and corrects one qubit error. This code can be described by the following map:

$$\begin{aligned} |0\rangle \mapsto |\overline{0}\rangle = \frac{1}{\sqrt{8}}\big(&|0000000\rangle + |1111000\rangle + |1100110\rangle + |1010101\rangle \\ &+ |0011110\rangle + |0101101\rangle + |0110011\rangle + |1001011\rangle \big) \\ |1\rangle \mapsto |\overline{1}\rangle = \frac{1}{\sqrt{8}}\big(&|0000111\rangle + |1111111\rangle + |1100001\rangle + |1010010\rangle \\ &+ |0011001\rangle + |0101010\rangle + |0110100\rangle + |1001100\rangle \big) \end{aligned} \tag{6}$$

From [7], we know that pure state erasure correcting codes are basically QSS schemes of maximal access structures. Now, let us distribute these 7 qubits among three different parties, A, B, C, and construct a $(2, 3)$ threshold scheme. Suppose that A has qubits $\{1, 2, 3, 4\}$, B has $\{5\}$ and C has $\{6, 7\}$. Since this is a pure QSS scheme, to prove its validity it suffices to prove that the density matrix of each unauthorized set is independent of the secret[7, 24]. Assume that we are going to share $|\psi_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. The shared secret can be described by state $|\overline{\psi_0}\rangle$, where $|\overline{\psi_0}\rangle = \alpha\,|\overline{0}\rangle + \beta\,|\overline{1}\rangle$. In this case, $\{A\}$, $\{B\}$ and $\{C\}$ are unauthorized. To compute the partial traces, it is useful to rewrite the logical qubits of Equation (6) as follows:

$$
\begin{aligned}
|0\rangle \mapsto |\overline{0}\rangle &= \frac{1}{2}\big(|G_{00}\rangle|000\rangle + |G_{12}\rangle|110\rangle + |G_{13}\rangle|101\rangle + |G_{23}\rangle|011\rangle\big) \\
|1\rangle \mapsto |\overline{1}\rangle &= \frac{1}{2}\big(|G_{00}\rangle|111\rangle + |G_{12}\rangle|001\rangle + |G_{13}\rangle|010\rangle + |G_{23}\rangle|100\rangle\big)
\end{aligned} \tag{7}
$$

where $|G_{00}\rangle$ is the four qubit GHZ state $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$ and $|G_{ij}\rangle$ is obtained from $|G_{00}\rangle$ by flipping the $i-$th and $j-$th qubit.

Thus, computing partial trace for every share produces the following density matrices which clearly are independent of the state $|\psi\rangle$:

$$
\rho_A = \mathrm{Tr}_{B,C}\left(\,|\bar{\psi}_0\rangle\langle\bar{\psi}_0|\,\right) = \frac{1}{4}\sum |G_{ij}\rangle\langle G_{ij}|, \quad \rho_B = \frac{1}{2}I_B, \quad \rho_C = \frac{1}{4}I_C \tag{8}
$$

Where I_B is the identity matrix of size 2 (over B's one qubit space) and I_C is the identity matrix of size 4 (over C's two qubit space). To obtain this results we used the condition that $|\alpha|^2 + |\beta|^2 = 1$.

Note that the authorized parties can recover the state, for example B and C can recover the secret by computing the parity bit of their shares (applying two CNOTs from fifth and sixth qubit to the last qubit, and then applying two CNOTs from the last qubit to the fifth and sixth qubit). In fact with this sequence of actions, the last three qubits transform as $|i, j, k\rangle \longrightarrow |j + k, i + k, i + j + k\rangle$ and hence

$$
\begin{aligned}
|\overline{0}\rangle &\mapsto |\xi\rangle \otimes |0\rangle \\
|\overline{1}\rangle &\mapsto |\xi\rangle \otimes |1\rangle
\end{aligned} \tag{9}
$$

where

$$
|\xi\rangle = \frac{1}{2}\big(|G_{00}\rangle|00\rangle + |G_{12}\rangle|11\rangle + |G_{13}\rangle|01\rangle + |G_{23}\rangle|10\rangle\big). \tag{10}
$$

Hence the shared state $\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$ transforms to $|\xi\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)$ and is retrieved. We will now describe how concatenation of this scheme will lead to other more general schemes.

3.1 An (n, n) QSS scheme

A number of (n, n) QSS schemes have already been proposed in different contexts such as [6, 21]. However most of these schemes use high-dimensional systems, which are not apt to the current schemes for actual quantum computation. Moreover, finding the right purification method for schemes that support universal quantum computation might not be straightforward. Thus, we are going to propose a new (n, n) scheme that satisfies our requirements.

Consider the (n, n) threshold scheme which obviously is not a maximal structure. Suppose the following hierarchy is applied to a secret state:

Starting from the bottom of the Fig. 5, we see that the players A_{n-1} and A_n can recover the state s_{n-2} which with the information supplied by A_{n-2} can lead to the recovery of the state in the upper level and so on until we reach the top of the figure where the collaboration of A_1 finally leads to the recovery of the encoded state. Note that in terms of quantum circuits, and in view of Equation (6) and the description following it on 7-qubit codes, a node like s_1 represents 4 qubits and the above figure implies that the 7-qubit code is applied to each one of the qubits in possession of s_1.

In this process, the shares D_1 to D_{n-1} are discarded, that is they are traced over. This is a reflection of the non-maximality of the (n, n) access structure and Corollary (2) of [7]. Instead of discarding

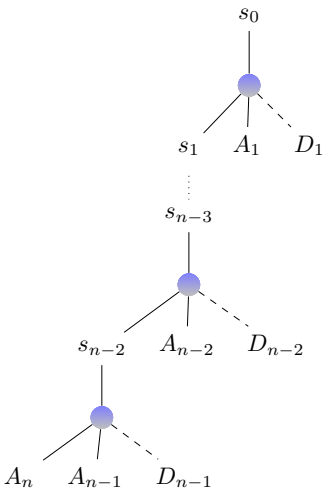

Figure 5: Hierarchical construction of the (n, n) threshold scheme.

these shares, one can assemble them and give them to a new member A_{n+1} according to the Fig. (6). This will then correspond to a new access structure, denoted by Ω_n which will be explained in the next subsection. According to theorem (3) of [7], this scheme, being maximal, can be implemented by sharing a pure state.

Remark. One might ask why a scheme formed by concatenating simpler quantum secret sharing schemes is also a (secure) quantum secret sharing scheme and why unauthorized subsets in this new scheme contain no information about the secret. It is easy to prove in the case of maximal access structures since if $S \notin \mathcal{A}(X)$ then we know $S^c \in \mathcal{A}(X)$ and S contains no information about the secret. In addition, for non-maximal access structures, it is possible to apply the same argument on the purified version of that scheme. This is explicitly proved in the Gottesman's work On the Theory of Quantum Secret Sharing [7].

3.2 A new access structure: The Ω_n scheme

The final building block that we need for constructing general access structures is a new and maximal access structure which we denote by Ω_n defined by its minimal authorized sets as

$$\Omega_n = \langle A_1 A_2 \dots A_n, A_1 A_{n+1}, A_2 A_{n+1}, \dots, A_n A_{n+1} \rangle \tag{11}$$

This means that any authorized set either contains A_{n+1} or contains all other shares. We call A_{n+1} the central share. Since this is a maximal access structure, from [7], a QSS scheme for it can be constructed by purifying an (n, n) scheme. When we consider our previous construction of (n, n) scheme, we achieved this construction by discarding $D_1, D_2, \dots, D_{n-1}$ from a pure state. Thus, if instead of discarding those shares, we produce a new share A_{n+1}, where $A_{n+1} = \{D_1, \dots, D_{n-1}\}$ we have effectively purified this scheme.

Same as before, $A_1 A_2 \dots A_n$ are able to recover the secret. In addition, A_{n+1} can also recover the secret with the help of one of the other shares with the same method (recovering from s_i to the top recursively).

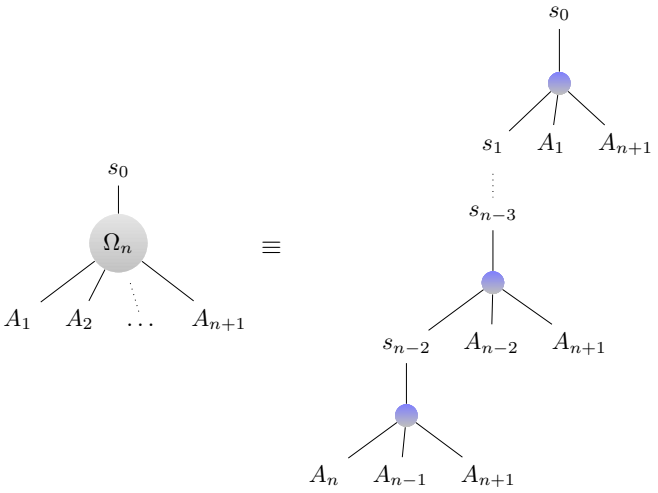

Figure 6: Hierarchical construction of the Ω_n access structure, eq. (11).

3.3 General schemes

Let us start with a simple case. Assume that the set is $X = \{A, B, C\}$ and the access structure is $\mathcal{A}_0(X) = \langle AB, AC\rangle$. In the classical case, to share a secret string of bits s, one makes two copies of it and share it together with random strings r_i according to the following scheme

$$\begin{aligned} A_1 &= s + r_1, \quad & B_1 &= r_2 \\ A_2 &= s + r_1', \quad & C_1 &= r_2' \end{aligned}$$

where $r_1 + r_2 = 0$ and $r_1' + r_2' = 0$. Here by A_1 and A_2 we mean the first and the second random string given to the player A.

When we come to quantum state sharing, due to limitations from the no-cloning theorem [26], we have to use a method similar to [7] and use the Ω_2 scheme introduced in subsection 3.2 as a substitute for copying. Fig. 7 is self-explanatory. Three shares are given to A, namely A_1, A_2 and A_3 and one share to each of B and C. The two shares D_1 and D_2 are redundant and are not used.

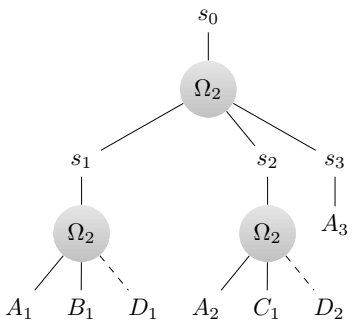

Figure 7: Hierarchical construction of the access structure $\mathcal{A}_0(X) = \langle AB, AC\rangle$. Note that Ω_2 is the same as the (2,3) access structure shown in previous figures with a blue bulb.

Starting from the bottom, AB can retrieve s_1 and then with the share A_3 (in possession of A) retrieve s_0. A similar path exists also for AC, but none for BC.

To construct the scheme for any access structure, we use induction. Assume that we already know how to construct all access structures with less than $n+1$ parties. Then we proceed with the following steps:

Case 1. $\mathcal{A}_{n+1}$ is maximal:

In this case, we remove an arbitrary player x from $\mathcal{A}_{n+1}$ turning it into a non-maximal structure $\mathcal{A}_n$. Then by Theorem (3) of [7], the state which achieves the structure $\mathcal{A}_n$ between these players is necessarily mixed, and any purification of this state has a unique $\mathcal{A}_{n+1}$ access structure. By purifying this mixed state and giving all the extra qubits which result from purification to the player x, we achieve a pure state sharing the state according to $\mathcal{A}_{n+1}$.

Example 2. Consider the set $X = \{A, B, C, E\}$ and the maximal structure $\overline{\mathcal{A}} = \langle AE, BE, CE, ABC\rangle$. To make a scheme for this, we remove A and turning it to $\overline{\mathcal{A}'} = \langle BE, CE\rangle$. The scheme for this is already known and given by Fig. 7, where D_1 and D_2 have been discarded. It is now enough to give these two shares to the removed player A. The final scheme is now given by Fig. 8.

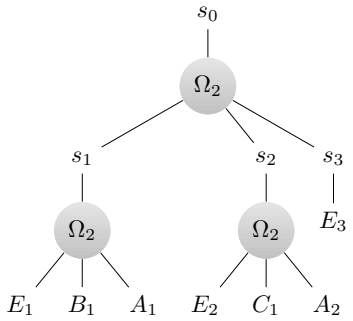

Figure 8: Constructing the access structure of example 2.

Case 2. $\mathcal{A}_{n+1}$ is not maximal:

In this case, it is obvious that the above method does not work, since if proceeded as above, the final state would be pure which according to Corollary (2) of [7] cannot correspond to $\mathcal{A}_{n+1}$ which is known to be a non-maximal access structure. Let this access structure be specified by its minimal authorized subsets $\langle T_1, T_2, \cdots T_r\rangle$ whose sizes are given by $|T_i| = k_i$. Obviously $|T_1 \cup T_2 \cup \cdots T_k| = n+1$. Consider the Fig. 9. Each of the states s_i can be recovered by each group T_i. However, this by itself should not lead to the recovery of s_0 (otherwise no cloning will be violated). To remedy this, we expand $\langle T_1, T_2, \cdots T_r\rangle$ by adding subsets to it in order to make it maximal. Denote this expanded structure by $\overline{\tilde{\mathcal{A}}}_{n+1}$. From case 1, we know how to share a secret s_c to this structure. Now since every T_i can recover its own secret s_i and through membership in $\overline{\tilde{\mathcal{A}}}_{n+1}$ it can also recover the central share s_c, then by the property of Ω_r, the secret s_0 can be recovered.

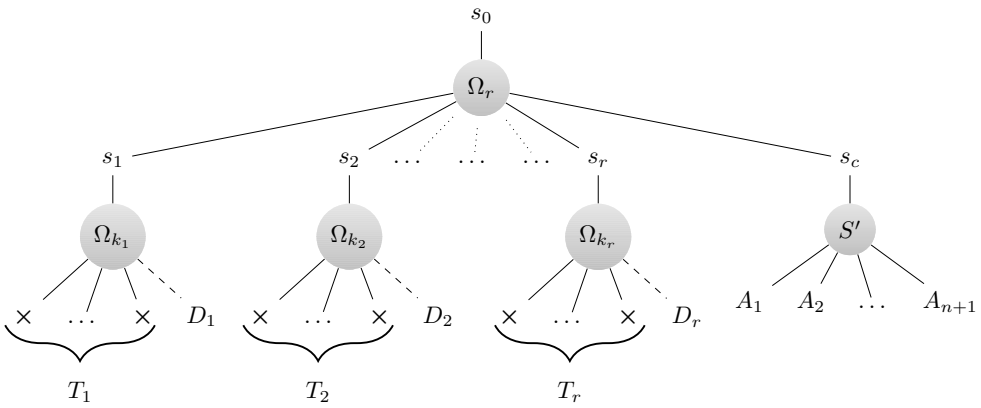

Figure 9: The induction step for the case when $\mathcal{A}_{n+1}$ is not maximal. See the description in **Case 2**

.

Remark. The reader may ask why we have used the Ω_{k_i} schemes in Fig. 9 to share s_i to the set T_i, while we could have also used any threshold scheme $(k_i\ ,\ k_i)$ for that purpose, for instance, the scheme that is proposed in [21], which also provides universal quantum computation. The reason is that the Ω_{k_i} schemes being maximal, lead to pure states and hence their concatenations will also be pure. Note that all non-maximal access structures are produced by discarding some shares (i.e. D_i's) from these pure concatenated schemes. Thus, in the purification step, one specific way of purification that also produces a concatenated 7-qubit code, is to include the discarded D_i's as a share of a new party member. This effectively purifies the non-maximal scheme.

Example 3. Consider again the set $X = \{A, B, C, E\}$ and the non-maximal access structure $\mathcal{A}_4 := \mathcal{A}(X) = \langle ABC, BE, AE\rangle$. This is not maximal (since neither AB nor CE are authorized). Therefore we follow the procedure of Fig. 10. The first step is to expand the secret using a Ω_3 scheme, and distribute the first three shares to the corresponding minimal authorized sets using Ω_n schemes:

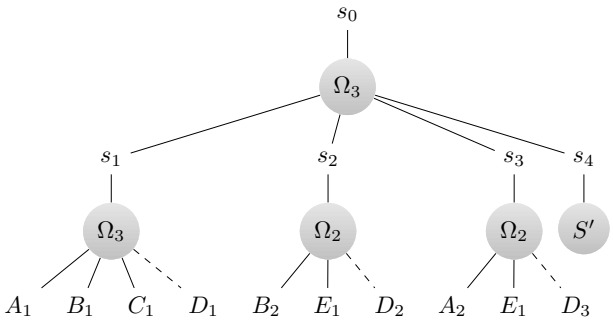

Figure 10: Construction of the access structure in example 3.

We then amend $\mathcal{A}$ to a maximal structure $\overline{\mathcal{A}} = \langle AE, BE, CE, ABC\rangle$ for which we know how to implement a QSS from Fig. 8. Putting these two figures together according to the general scheme Fig. 9, we obtain the scheme in Fig. 11.

The reader can now verify that every authorized set in $\langle BE, AE, ABC\rangle$ can retrieve the secret and none of the unauthorized set can reach s_0.

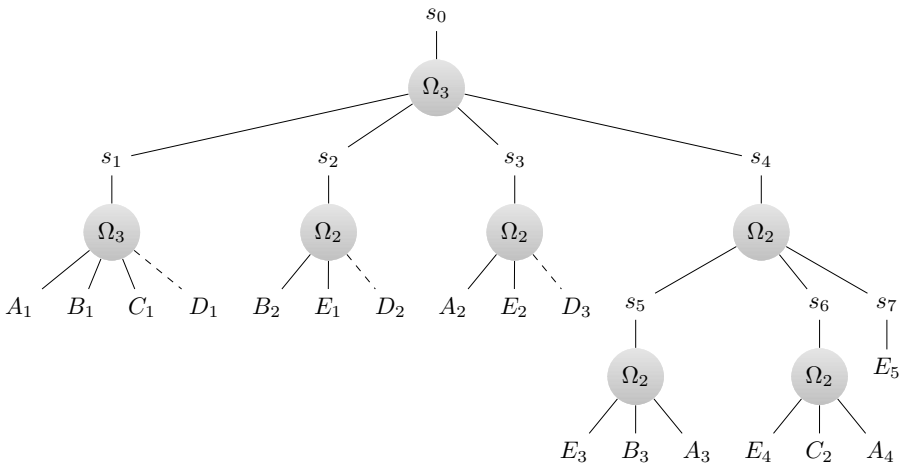

Figure 11: Construction of the access structure in example 3.

4 Computing on shared secrets

We have managed to share a qubit state according to any access structure among a set of players. The construction is all based on sharing a 7-qubit code in a concatenated scheme. To do universal quantum computation on these access structures, it is then enough to adopt the known techniques for doing quantum computation on 7-qubit codes. We begin with a description of universal gates on the 7-qubit code.

4.1 Computing on the 7-qubit codes

It is well-known [25] that the logical Pauli operators, the Hadamard and the CNOT gate can be implemented on the 7-qubit code, by their bit-wise transversal operation, that is:

$$\overline{X_a} = {X_a}^{\otimes 7}, \qquad \overline{H} = H^{\otimes 7}, \qquad \overline{\text{CNOT}} = \text{CNOT}^{\otimes 7}, \tag{12}$$

where X_a is any Pauli operator and in the last relation, all the 7 bits of the first logical state are the control bit and all the 7 bits of the second logical state are the target bits.

Verification of relation for the X and Z Pauli operators is simple and easily verified by looking at the structure of the logical qubit states $|\overline{0}\rangle$ and $|\overline{1}\rangle$ in Equation (6). The relation for Hadamard operator and CNOT is proved [25] by noting that the stabilizers of the 7-qubit code and in fact any self-dual CSS code is either the product of X operators or Z operators in similar positions. In other words, the logical CNOT realized as $\overline{\text{CNOT}} = \text{CNOT}^{\otimes 7}$ has the same commutation relations with $\overline{X}$ and $\overline{Z}$ as the ordinary CNOT has with X and Z.

We also need to implement the gate $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ which transforms the eigenstates of the X operator to that of the Y operator. In view of the structure of the logical states $|\overline{1}\rangle$ and $|\overline{0}\rangle$ in Equation (6) (i.e. the number of 1's in these states), it is obvious that we can implement the logical $\overline{S}$ gate as

$$\overline{S} = {S^\dagger}^{\otimes 7}. \tag{13}$$

To make this set a universal set of gates, we have to include the $\frac{\pi}{8}$ gate, $\overline{T} = |\overline{0}\rangle\langle\overline{0}| + e^{i\pi/4}\,|\overline{1}\rangle\langle\overline{1}|$. However, the problem is that this gate cannot be implemented directly and transversally as with the previous gates. To do this, we use gate teleportation [28, 29] as shown in Fig. 12, which explains the teleportation of the T gate on one-qubit unencoded states.

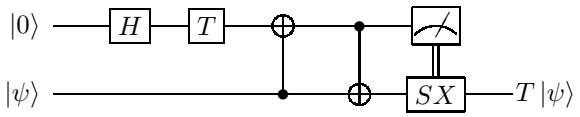

Figure 12: Gate teleportation of the T-gate on one-qubit.

The state evolved through this circuit after the operation of the two CNOT gates is given by ($|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$):

$$|0\rangle \otimes \Big(\alpha\,|0\rangle + \beta e^{i\pi/4}\,|1\rangle\Big) + |1\rangle \otimes \Big(\beta\,|0\rangle + \alpha e^{i\pi/4}\,|1\rangle\Big). \tag{14}$$

Upon measuring the ancilla (first qubit) the second qubit projects either onto the state $T|\psi\rangle$ or to a state which is corrected by the gate SX to $T|\psi\rangle$. In either case the gate T is teleported by using the Hadamard gates, the CNOT and the S and the X gates.

We now upgrade this circuit and adapt it to the present setting for implementation of the encoded $\overline{T}$ on logical states. (Fig. 13)

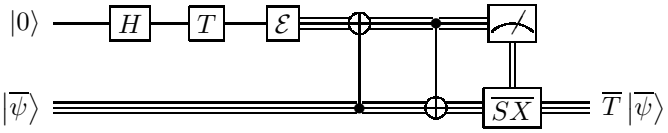

Figure 13: Gate teleportation of the encoded $\overline{T}$-gate on logical states

We assume that a number of ancillary states are prepared in state $TH\,|0\rangle$, and are pre-shared among party members using the same QSS scheme. The box $\mathcal{E}$ shows the encoding circuit which encodes qubit states $|0\rangle$ and $|1\rangle$ to logical states $|\overline{0}\rangle$ and $|\overline{1}\rangle$. The output of the circuit is now given by

$$|\overline{0}\rangle \otimes \Big(\alpha\,|\overline{0}\rangle + \beta e^{i\pi/4}\,|\overline{1}\rangle\Big) + |\overline{1}\rangle \otimes \Big(\beta\,|\overline{0}\rangle + \alpha e^{i\pi/4}\,|\overline{1}\rangle\Big) \tag{15}$$

which shows that the output state is now given by $\overline{T}|\overline{\psi}\rangle$ provided that we can do the correction $\overline{SX}$ which we obviously can. The only problem is to see if by separable qubit-wise measurement we can determine the first logical qubit to be in $|\overline{0}\rangle$ or $|\overline{1}\rangle$. This is indeed possible by checking the parity of the 7-bits measured by the players as seen from Equation (6). Note that at some point in the hierarchy we might need to discard one of the shares of the $(2, 3)$ scheme constructed by the 7-qubit code. To make measurement possible based on the parity of bit-wise measurements, we need to discard the first four qubits while discarding one share. This also comes from Equation (6). Otherwise, the overall measurement result of bit-wise measurement is important for measuring the logical Z gate. For example, getting 00001 for the first two shares means that we need to apply correction. In this way, we have shown that by transversal bitwise gate operations and measurements, it is possible to do universal quantum computation on the 7-qubit code and hence do quantum computation on a $(2, 3)$ scheme which is the basic building block of general access structures. Before proceeding to the computation, a note on security of the protocol, the difficulty of gaining information by unauthorized subsets, is in order.

4.1.1 A note on security

First we should stress that even in the field of classical cryptography, few protocols are proved to be information theoretically secure, rather most of them are proved to be practically secure in view of the large resources needed for their breaking. In the present case, the assumption is that in the purified version of any scheme, which results in a maximal access structure, at least one authorized set is not dishonest. Furthermore, we assume that the shared state is completely secure after the sharing process, which means this proof will not work if the original state is tampered with, i.e. if is entangled with some qubits in possession of the dishonest party. Given this, let us consider a scenario in which a dishonest party tries to gain information about the secret by applying arbitrary operators and measurements during the computation. This would effectively disturb the information contained in its complement set [30], leading to the revealing of the unauthorized leakage of information. We prove this statement for maximal access structures, since any non-maximal access structure can be described by a maximal access structure with one share discarded [7]. In maximal access structures, the complement of a dishonest party, which is not authorized, is an authorized set [7]. In addition, from equations (6 and 15) we see that during the application of a T gate, any information shared between these two group is independent of the secret. The reason is that when written in the computational basis, the overall shared bits belong to the logical 0 or logical 1 sub-spaces each with probability $\frac{1}{2}$ and independent of their share. Therefore no additional information is leaked to the dishonest party. At each step, the density matrix of the dishonest party remains independent of the secret since every operation is local and the authorized party should be able to recover the secret by following the protocol. This proves our claim.

4.2 Computing on general access structures

Generalizing universal quantum computation on 7-qubit code to any access structure is now straightforward since the latter is made from the concatenation of the former. The problem in our context is simpler than the one in [25] which is devoted to fault-tolerant computation since in our case a basic step is to measure the logical Z operator as explained in subsection 4.1, which need not be fault-tolerant. Assume that some n qubit secret $|s\rangle$ is shared among n parties using a scheme that is implemented as explained in subsection 3.3, with access structure S. Note that every qubit i is shared independently. Furthermore, we use the same assumption as in [21] for doing computation on QSS schemes. We assume that the desired circuits require less than t number of T gates in general. Thus, by pre-sharing t number of $\tau = TH\,|0\rangle$ states, the encoding step is finished.

The next step is expanding our computation method while we expand a qubit in a hierarchy. We already know how to do transversal computation on 7-qubit code and a discarded 7-qubit code). As for any concatenated quantum code, each qubit has to apply a relevant gate according to its parent (the node above it in the diagram). Thus, while expanding a qubit using a 7-qubit code, it is obvious that $X, Z,$ CNOT, H can still be implemented transversally. However, S gate and Z-measurement require more explanation. As for the S gate, since $\overline{S} = {S^\dagger}^{\otimes 7}$ and $\overline{S^\dagger} = S^{\otimes 7}$ each new qubit can determine the appropriate gate based on its parent. Hence, qubits at an odd level have to apply the $S^\dagger$ gate, and qubits at an even level have to apply the S gate. Furthermore, since measuring Z operator on an expanded ancillary qubit can be done by computing the parity bit of bit-wise measurements (if we use the last 3 qubits of 7-qubit code as a $(2, 2)$ scheme) the overall parity bit can still determine whether there is a need for applying the correction SX operator. Note that these measurements (even in the previous subsection) destroy any superposition of encoded ancillary state, which causes no problem in this context since these states have no use after the measurement.

Hence, the only modification needs to be done in the computation method for general access structures from the 7-qubit code is the application of the S gate. Using this method, we are able to

apply arbitrary quantum circuits with at most t number of T gates in their construction. However, as mentioned in [21], there is still the possibility that party members might be able to use a protocol to produce these shared ancillary τ states on demand.

5 Conclusion and Outlook

We proposed a method to construct QSS schemes for general access structures using only qubits, on which we are also able to do universal quantum computation with transversal opertions and pre-shared ancillary states. Our method only uses basic blocks of $(2, 3)$-threshold scheme in contrast to more complicated (k, n)-threshold scheme mentioned in [7]. The ease of computation is because our method is based on 7-qubit code, which also enables us to do experiments on more complex access structures with the current state of experimental quantum computation. These schemes might use exponential number of qubits depending on the access structure because of the purification steps. However, similar ideas might be used to construct usefull schemes such as threshold schemes more efficiently using concatenation of simple error correcting codes. It might also be possible to do a form of blind quantum computation using methods similar to other secure protocols [21, 31]

6 Acknowledegments

We thank the referees, specially one of them, whose very careful reading of the manuscript and very valuable comments led to a much better presentation of this article. This work was done with a support from the research council of the Sharif University of Technology, and with the financial support from Sharif University of Technology under grant no. G951418, and with partial support from Iran National Science Foundation under the grant INSF-96011347.

References

[1] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[2] G. R. Blakley et al. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, pages 313–317, 1979.

[3] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3):1829, 1999.

[4] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Physical Review A*, 59(1):162, 1999.

[5] A. D. Smith. Quantum secret sharing for general access structures. *arXiv preprint quant-ph/0001087*, 2000.

[6] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648–651, Jul 1999.

[7] D. Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000.

[8] H. Imai, J. Müller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter. A quantum information theoretical model for quantum secret sharing schemes. *arXiv preprint quant-ph/0311136*, 2003.

[9] C.-M. Bai, Z.-H. Li, T.-T. Xu, and Y.-M. Li. A generalized information theoretical model for quantum secret sharing. *International Journal of Theoretical Physics*, 55(11):4972–4986, 2016.

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, Jan 1992.

[11] S. Grblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger. Experimental quantum cryptography with qutrits. *New Journal of Physics*, 8(5):75, 2006.

[12] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han. Simple implementation of quantum key distribution based on single-photon bell-state measurement. *Phys. Rev. A*, 92:012319, Jul 2015.

[13] A. Broadbent, J. Fitzsimons, and E. Kashefi. Proceedings of the 50th annual ieee symposium on foundations of computer science. 2009.

[14] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

[15] Y. Ouyang, S.-H. Tan, and J. F. Fitzsimons. Quantum homomorphic encryption from quantum codes. *Phys. Rev. A*, 98:042334, Oct 2018.

[16] V. Karimipour and M. Asoudeh. Quantum secret sharing and random hopping: Using single states instead of entanglement. *Phys. Rev. A*, 92:030301, Sep 2015.

[17] S. Bagherinezhad and V. Karimipour. Quantum secret sharing based on reusable greenberger-horne-zeilinger states as secure carriers. *Phys. Rev. A*, 67:044302, Apr 2003.

[18] X.-L. Song, Y.-B. Liu, H.-Y. Deng, and Y.-G. Xiao. (t, n) threshold d-level quantum secret sharing. *Scientific Reports*, 7(1):6366, 2017.

[19] G. Gordon and G. Rigolin. Generalized quantum-state sharing. *Physical Review A*, 73(6):062316, 2006.

[20] H. Qin and Y. Dai. Proactive quantum secret sharing. *Quantum Information Processing*, 14(11):4237–4244, 2015.

[21] Y. Ouyang, S.-H. Tan, L. Zhao, and J. F. Fitzsimons. Computing on quantum shared secrets. *Physical Review A*, 96(5):052333, 2017.

[22] B. Fortescue and G. Gour. Reducing the quantum communication cost of quantum secret sharing. *IEEE Transactions on Information Theory*, 58(10):6659–6666, 2012.

[23] C.-M. Bai, Z.-H. Li, M.-M. Si, and Y.-M. Li. Quantum secret sharing for a general quantum access structure. *The European Physical Journal D*, 71(10):255, 2017.

[24] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, Mar 2000.

[25] D. Gottesman. Stabilizer codes and quantum error correction. *arXiv preprint quant-ph/9705052*, 1997.

[26] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[27] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[28] D. Gottesman and I. L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390, 1999.

[29] X. Zhou, D. W. Leung, and I. L. Chuang. Methodology for quantum logic gate construction. *Phys. Rev. A*, 62:052316, Oct 2000.

[30] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[31] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner. Composable security of delegated quantum computation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–425. Springer, 2014.