arXiv:1801.02445v1 [quant-ph] 8 Jan 2018

# Computing on Quantum Shared Secrets for General Access Structures

Roozbeh Bassirian[1], Sadra Boreiri[1], 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**

We introduce a method for performing universal quantum computation on quantum states shared according to general access structures. This generalizes recent attempts for doing quantum computation on $(n, n)$ threshold schemes. In a general access structure certain authorized subsets, depending on their weights, can retrieve a secret shared state, and only by their collaboration universal quantum computation can be performed on the shared state. To achieve this we have used concatenation of seven-qubit codes.

## 1 Introduction

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. Furthermore suppose that she wants to perform universal quantum computation on this state by enquiring participants to perform local actions on their share, without retrieving (or decoding) the state by the legitimate parties. There has been recent reports in achieving this task for certain threshold schemes [17]. The question is how it can be performed for general access structures.

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 [1, 2, 3], and even commercialized, new ones with different domains of applications are being proposed. Blind quantum computation [4, 5], quantum homomorphic encryption [6], sharing of classical data [7, 8, 9] and quantum states [10, 11, 12] and even performing quantum computation on shared secrets [17] are good examples of these protocols.

The latter refers to schemes where a classical message or a quantum state is shared between $n$ parties such that it can be recovered only by the collaboration of all the parties [17]. This is the most common and the simplest access structure, denoted by $(n, n)$. It generalizes to the $(k, n)$ access structure, where any subset of size $k$ can recover the data by collaboration [11]. However, there are many applications where the members do not have an equal level of authorization. Therefore the most general access structure is where only certain subsets of the set of receivers can retrieve the classical or the quantum data.

While there have been a lot of progress in quantum state sharing (QSS) schemes for $(n, n)$ schemes and threshold schemes $(k, n)$, much less has been reported on these schemes for general access structures. In this respect we can mention [11, 12], where the theory of QSS is connected to the theory of quantum error correction and general access structures are constructed inductively. At each step, new access structures are constructed by either expansion of previous shares using threshold schemes[11](using polynomial codes[13]), or purification of mixed quantum sharing schemes. However, the point is that in these schemes the dimension $d$ of the $d$-level system required for construction of threshold schemes grows relative to the number of party members. In addition, while 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.

Of particular interest to us are the works [12] where sharing of a state according to a general access structure is discussed and the recently proposed scheme [17], where quantum computation is performed on a secret shared according to a $(n, n)$ scheme. In this method, a quantum circuit is applied on shared secrets by the collaboration of all party members. While the desired quantum circuit is known by every party member, no information is leaked about the input and hence the output secret state to the un-authorized parties during the computation. For performing the known circuit, 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.

The aim of our work is to construct QSS schemes for general access structures using qubits, in a manner that makes distributed quantum computation possible. We use the same induction steps proposed in [12]. However, in all the steps we use new QSS schemes based on seven-qubit code as building blocks, and we specify the purification method explicitly making distributed quantum computation possible for these schemes. It is worth mentioning that using our purification method, it is also possible to do universal quantum computation on the QSS schemes proposed in [12]. However, it would require ancillary states for every gate. The advantage of using seven-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[19] and stabilizer formalism[15]. 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 subsets of $X$ with the property that it should be **monotone**.

This means that if $S$ belongs to $\mathcal{A}(X)$, then any superset $T$ of $X$ (i.e. any set $T$ where $S \subset T$) should also belong to $\mathcal{A}(X)$. This is simply the reflection of a natural property that if a subset $S$ is authorized, any other subset containing $S$ should also be authorized. In quantum state sharing an extra condition is imposed on the access structure which comes from the no-cloning theorem: For every two authorized sets $S$ and $T$, $S \cap T \neq \emptyset$. Hereafter, whenever we mention access structure, we mean those which have this property. Also for the brevity of notations, a subset like $\{A, B, C\}$ is denoted simply by $ABC$.

**Definition 2.** An access structure $\mathcal{A}$ is usually denoted by its **minimal authorized sets** and denoted by $\mathcal{A} = \langle T_1, T_2, \cdots T_r \rangle$, where $T_i$'s all the sets which generate $\mathcal{A}$ by which we mean that all the larger sets which are supersets of $T_i$'s are eliminated. For example $\mathcal{A} = \{AB, AC, ABC\} = \langle AB, AC \rangle$.

We use the notation of $(k, n)$ for threshold schemes, which basically refers to an access structure in which every subset of at least $k$ party members is authorized. Of special importance are the class of **maximal** access structures.

**Definition 3.** [12] For a set $X$, an access structure is maximal and denoted by $\overline{\mathcal{A}}(X)$ if ,for every subset $S \in X$, either $S$ or the complement of $S$ is authorized.

For example, the threshold schemes $(n, n)$ are not maximal, while a $(2, 3)$ scheme is 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 $|\overline{\psi}\rangle = \alpha|\overline{0}\rangle_{\overline{X}} + \beta|\overline{1}\rangle_{\overline{X}}$ 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).

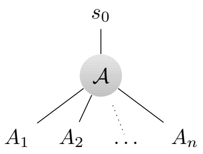

Figure 1

**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. Which means 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 the special figure (where there is no symbol on the bulb):

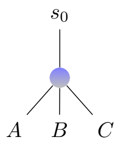

Figure 2

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.

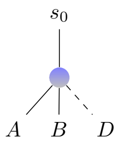

Figure 3

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 $\rho_{AB}$. 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

$$\mathcal{R}_{_{AB}}(|\overline{\psi}\rangle_{_{ABD}}\langle\overline{\psi}|) = |\psi\rangle_{_A}\langle\psi| \otimes \chi_{_{BD}} \tag{1}$$

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:

$$\mathcal{R}_{_{AB}}\left(tr_{_D}(|\overline{\psi}\rangle_{_{ABD}}\langle\overline{\psi}|)\right) = |\psi\rangle_{_A}\langle\psi| \otimes tr_{_D}\chi_{_{BD}} \tag{2}$$

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 [12]. As an example consider the following figure, 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 [12]. For example, in Figure (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.

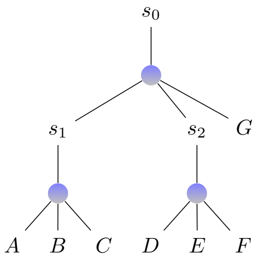

Figure 4

# 3 Quantum state sharing using 7-qubit code

We will construct all the QSS schemes from a basic threshold (2,3) scheme which is based on using the 7-qubit code. The seven-qubit code is a $[[7, 1, 3]]$ CSS code[14], that uses the classical $[7, 4, 3]$ hamming code to generate its stabilizers[15]. This code can be described by the following map:

$$\begin{aligned} |0\rangle \mapsto \left|\overline{0}\right\rangle &= |0000000\rangle + |1111000\rangle + |1100110\rangle + |1010101\rangle \\ &+ |0011110\rangle + |0101101\rangle + |0110011\rangle + |1001011\rangle \\ |1\rangle \mapsto \left|\overline{1}\right\rangle &= |0000111\rangle + |1111111\rangle + |1100001\rangle + |1010010\rangle \\ &+ |0011001\rangle + |0101010\rangle + |0110100\rangle + |1001100\rangle \end{aligned} \tag{3}$$

Please note that we are ignoring the normalization factor for ease of calculations. From [12], 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 $\{6, 7\}$. To prove that this is a secret sharing scheme since this is a pure QSS scheme, it suffices to prove that the density matrix of each unauthorized set is independent of the secret[12, 19]. Assume that we are going to share $|\psi_0\rangle = \alpha |0\rangle + \beta |1\rangle$. The shared secret can be described by state $\left|\overline{\psi_0}\right\rangle$, where $\left|\overline{\psi_0}\right\rangle = \alpha \left|\overline{0}\right\rangle + \beta \left|\overline{1}\right\rangle$. In this case, $\{A\}$, $\{B\}$ and $\{C\}$ are unauthorized. To compute the partial traces, it is useful to rewrite the logical qubits of Equation (3) as follows:

$$\begin{aligned} |0\rangle \mapsto \left|\overline{0}\right\rangle &= |G_{00}\rangle|000\rangle + |G_{12}\rangle|110\rangle + |G_{13}\rangle|101\rangle + |G_{23}\rangle|011\rangle \\ |1\rangle \mapsto \left|\overline{1}\right\rangle &= |G_{00}\rangle|111\rangle + |G_{12}\rangle|001\rangle + |G_{13}\rangle|010\rangle + |G_{23}\rangle|100\rangle \end{aligned} \tag{4}$$

where $|G_{00}\rangle$ is the four qubit GHZ state $|0000\rangle + |1111\rangle$ and $|G_{ij}\rangle$ is obtined 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 $|\psi\rangle$:

$$\begin{aligned} \rho_A = \mathrm{tr}_{B,C}(|\bar{\psi_0}\rangle\langle\bar{\psi_0}|) &= \sum_{i,j} |G_{ij}\rangle\langle G_{ij}|, \\ \rho_B &= I_B, \\ \rho_C &= I_C, \end{aligned} \tag{5}$$

where we have used the condition $|\alpha|^2 + |\beta|^2 = 1$.
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

$$\begin{aligned} |\overline{0}\rangle &\mapsto |\xi\rangle \otimes |0\rangle \\ |\overline{1}\rangle &\mapsto |\xi\rangle \otimes |1\rangle \end{aligned} \tag{6}$$

where

$$|\xi\rangle = |G_{00}\rangle|00\rangle + |G_{12}\rangle|11\rangle + |G_{13}\rangle|01\rangle + |G_{23}\rangle|10\rangle. \tag{7}$$

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 A $(n, n)$ QSS scheme

A number of $(n, n)$ QSS schemes have already been proposed in different contexts such as [11, 17]. However most of these schemes use high-dimensional systems, which would require more ancillary states for doing 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. We already know from [12] that concatenated QSS schemes is also a QSS scheme. Suppose the following hierarchy is applied to a secret state:

Starting from the bottom of the figure, 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 (3) 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 [12]. Instead of discarding these shares, one can assemble them and give them to a new member $A_{n+1}$ according to the following figure. This will then correspond to a new access structure, denoted by $\Omega_n$ which will be explained in the next subsection. According to theorem (3) of [12], this scheme, being maximal, can be implemented by sharing a pure state.

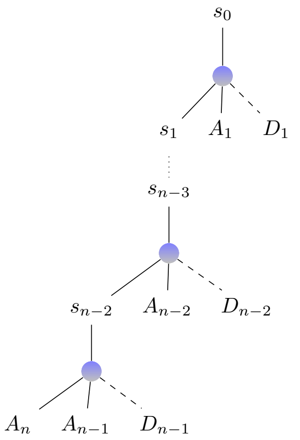

Figure 5

### 3.2 A new access structure: The $\Omega_n$ scheme

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

$$\Omega_n = \langle A_1 A_2 \dots A_n, A_1 A_{n+1}, A_2 A_{n+1}, \dots, A_n A_{n+1} \rangle \tag{8}$$

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 [12], 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.

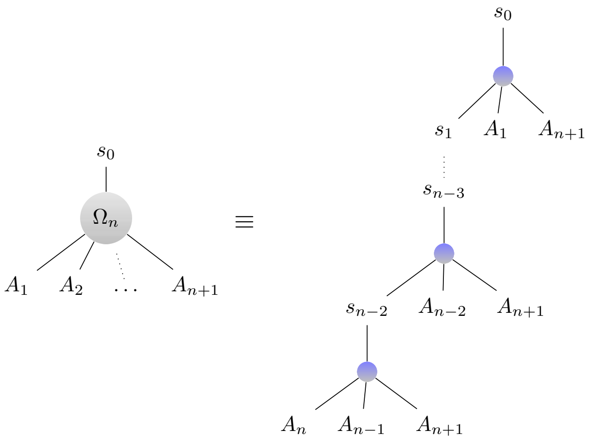

Figure 6

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).

### 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 $r_1' + r_2' = 0$. However, in quantum state sharing, due to limitations from the no-cloning theorem [16], we use a method similar to [12]. We use the $\Omega_3$ scheme introduced in subsection 3.2 as a substitute for copying. The following figure 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. Starting from the bottom, $AB$ can retrieve $s_1$ and then with the share $A_3$ (in procession 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:

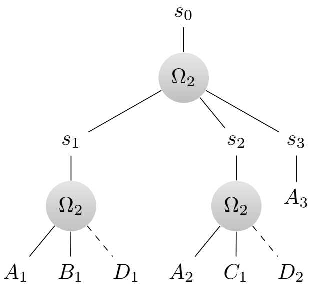

Figure 7

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

In this case, we remove one player say $x$ from $\mathcal{A}_{n+1}$ turning it into a non-maximal structure $\mathcal{A}_n$. Then by Theorem (3) of [12], 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 1.** 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 figure (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 Figure (8).

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

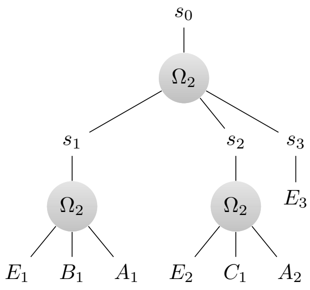

Figure 8

In this case, it is obvious that the above method does not work, since if proceed as above, the final state would be pure which according to Corollary (2) of [12] 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 Figure (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 $\Omega_r$, the secret $s_0$ can be recovered.

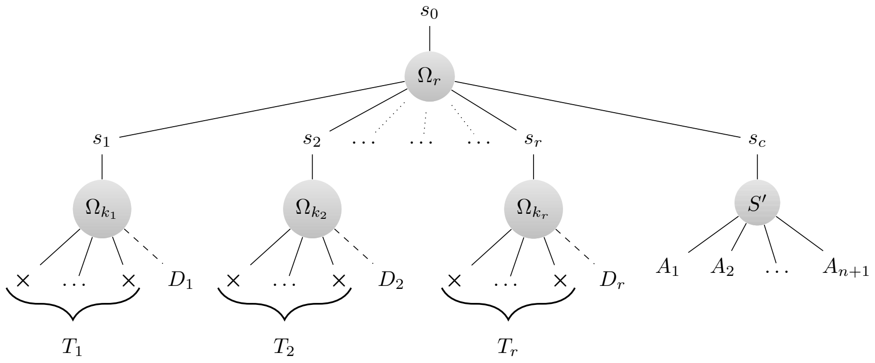

Figure 9

**Remark.** The reader may ask why we have used the $\Omega_{k_i}$ schemes in Figure (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 [17], which also provides universal quantum computation. The reason is that the $\Omega_{k_i}$ 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 seven-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 2.** Consider again the set $X = \{A, B, C, E\}$ and the access structure non-maximal 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 Figure (10). The first step is to expand the secret using a $\Omega_3$ scheme, and distribute the first three shares to the corresponding minimal authorized sets using $\Omega_n$ schemes:

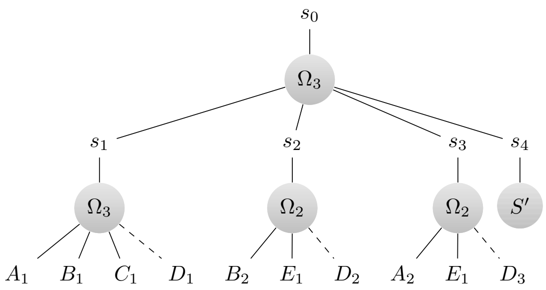

Figure 10

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 figure (8). Putting these two figures together according to the general scheme (9), we obtain the scheme in figure (11).

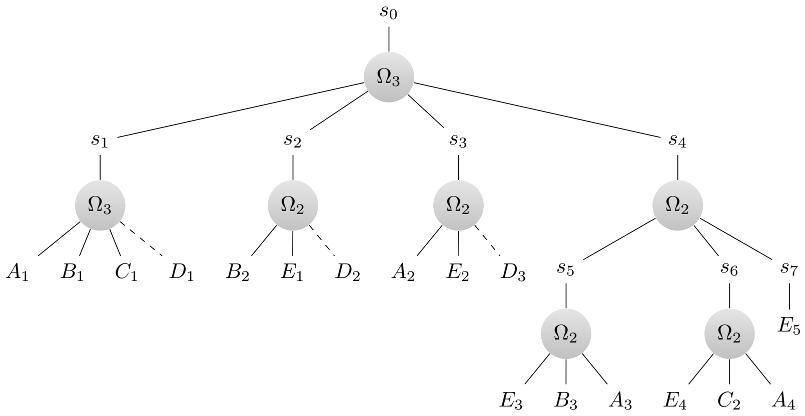

Figure 11

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 $s_0$.

# 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 seven-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 seven-qubit codes. We begin with a description of universal gates on the 7-qubit gate.

## 4.1 Computing on the 7-qubit codes

It is well-known [15] 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:

$$\overline{X_a} = {X_a}^{\otimes 7}, \qquad \overline{H} = H^{\otimes 7}, \qquad \overline{CNOT} = CNOT^{\otimes 7}, \tag{9}$$

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 (3). The relation for Hadamard operator and CNOT is proved [15] 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 $\overline{CNOT} = CNOT^{\otimes 7}$ 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 (3) (i.e. the number of 1's in these states), it is obvious that we can implement the logical $\overline{S}$ gate as

$$\overline{S} = {S^{\dagger}}^{\otimes 7}. \tag{10}$$

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 [21, 22] as shown in the following figure which explains the teleportation of the $T$ gate on one-qubit unencoded states.

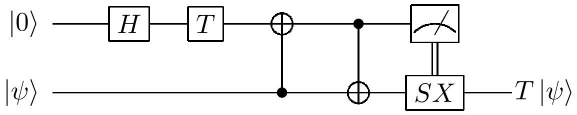

Figure 12

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

$$|0\rangle \otimes \Big(\alpha\,|0\rangle + e^{i\pi/4}\,|1\rangle\Big) + |1\rangle \otimes \Big(\beta\,|0\rangle + \alpha e^{i\pi/4}\,|1\rangle\Big). \tag{11}$$

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.

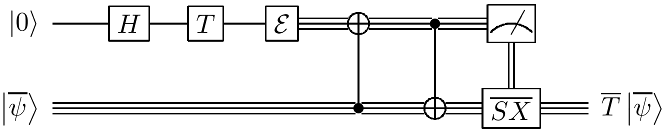
$|0\rangle$
H
T
$\mathcal{E}$
$|\overline{\psi}\rangle$
SX
$\overline{T}\,|\overline{\psi}\rangle$

Figure 13

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

$$\left|\overline{0}\right\rangle \otimes \left(\alpha\left|\overline{0}\right\rangle + e^{i\pi/4}\left|\overline{1}\right\rangle\right) + \left|\overline{1}\right\rangle \otimes \left(\beta\left|\overline{0}\right\rangle + \alpha e^{i\pi/4}\left|\overline{1}\right\rangle\right) \tag{12}$$

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 $\left|\overline{0}\right\rangle$ or $\left|\overline{1}\right\rangle$. This is indeed possible by checking the parity of the 7-bits measured by the players as seen from Equation (3). 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 seven-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 (3). 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.

Furthermore, it is possible to prove that at any step during the computation, any unauthorized dishonest party cannot gain any information about the secret. It is also possible to prove this statement by computing the density matrix of the overall state after each step as stated in [17]. However, it is easier to prove this statement from the perspective of erasure-correcting codes [12]. 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 [12]. In maximal access structures, the complement of a dishonest party, which is not authorized, is an authorized set [12]. In addition, from Equations (3, 12) any information shared between these two group of people during application of a $T$ gate is independent of the secret, and provides no additional information to the dishonest party. Thus, at each step, the density matrix of the dishonest party remains independent of the secret since every operation is local. Hence, any information gained about the secret by any dishonest party applying arbitrary operators and measurements during the computation would effectively disturb the information contained in the complement set [20]. Since the complement is authorized and is able to recover the secret, this leads to a contradiction.

## 4.2 Computing on general access structures

Generalizing universal quantum computation on seven-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 [15] 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 secret $|s\rangle = |\phi_1\phi_2 \dots \phi_s\rangle$ 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 $|\phi_i\rangle$ is shared independently using this method and results in an encoded shared state $\left|\overline{\phi_i}\right\rangle$. Furthermore, we use the same assumption as in [17] 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 $\tau = TH\left|0\right\rangle$ 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 seven-qubit code and a discarded seven-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 seven-qubit code, it is obvious that $X, Z, \text{CNOT}, H$ 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 seven-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 seven-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 [17], there is still the possibility that party members might be able to use a protocol to produce these shared ancillary $\tau$ states on demand.

# 5 Conclusion and Outlook

We proposed a method to construct QSS schemes for general access structures, on which we are also able to do universal quantum computation. However, these schemes require an exponential number of qubits because of the purification steps. The question remains open whether there exist a general scheme with a polynomial number of qubits. Moreover, we do not rule out the possibility that choosing more suitable basic blocks ($\Omega_n$ in our context) might reduce the number of qubits required to construct general access structures. Finally, while doing computation on these schemes, all participants know the exact circuit. The question remains open as to what extent it is possible to hide this information from participants, i.e. to do some sort of blind quantum computation.

# 6 Acknowledgements

This work was done with a support from the research council of the Sharif University of Technology.

# References

[1] Bennett, C.H., Bessette, F., Brassard, G. et al. J. Cryptology (1992) 5: 3. https://doi.org/10.1007/BF00191318

[2] Simon Groeblacher, Thomas Jennewein, Alipasha Vaziri, Gregor Weihs, Anton Zeilinger, New J. Phys. 8 (2006)

[3] Wen-Ye Liang, Mo Li, Zhen-Qiang Yin, Wei Chen, Shuang Wang, Xue-Bi An, Guang-Can Guo, and Zheng-Fu Han Phys. Rev. A 92, 012319 (2015)

[4] Anne Broadbent, Joseph Fitzsimons, Elham Kashefi, Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), pp. 517-526

[5] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F. Fitzsimons, Anton Zeilinger, Philip Walther, Science 20 Jan 2012: Vol. 335, Issue 6066, pp. 303-308 DOI: 10.1126/science.1214707

[6] Y. Ouyang, S.-H. Tan, and J. Fitzsimons. Quantum homomorphic encryption from quantum codes, August 2015. arXiv:1508.00938.

[7] V. Karimipour and M. Asoudeh, Phys. Rev. A 92, 030301(R) (2015)

[8] Saber Bagherinezhad and Vahid Karimipour Phys. Rev. A 67, 044302 (2003)

[9] Xiu-Li Song, Yan-Bing Liu, Hong-Yao Deng, Yong-Gang Xiao, Scientific Reports 7, Article number: 6366 (2017) doi:10.1038/s41598-017-06486-4

[10] Adam D. Smith, arXiv preprint quant-ph/0001087, (2000)

[11] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo Phys. Rev. Lett. 83, 648 (1999)

[12] Daniel Gottesman Phys. Rev. A 61, 042311 (2000)

[13] D. Aharonov, M. Ben-Or, Proceeding STOC '97 Proceedings of the twenty-ninth annual ACM symposium on Theory of computing (1997)

[14] A. R. Calderbank, Peter W. Shor, Phys. Rev. A 54, 1098 (1996)

[15] Daniel Gottesman, preprint arXiv:quant-ph/9705052 (1997)

[16] W. K. Wootters, W. H. Zurek, Nature 299, 802803 (1982)

[17] Yingkai Ouyang, Si-Hui Tan, Liming Zhao, and Joseph F. Fitzsimons Phys. Rev. A 96, 052333 (2017)

[18] Gottesman D. (1999) Fault-Tolerant Quantum Computation with Higher-Dimensional Systems. In: Williams C.P. (eds) Quantum Computing and Quantum Communications. Lecture Notes in Computer Science, vol 1509. Springer, Berlin, Heidelberg

[19] Emanuel Knill, Raymond Laflamme, and Lorenza Viola Phys. Rev. Lett. 84, 2525 (2000)

[20] Charles H. Bennett, Gilles Brassard, and N. David Mermin, Phys. Rev. Lett. 68, 557(1992)

[21] Daniel Gottesman, Isaac L. Chuang, Nature 402, 390393 (1999)

[22] Xinlan Zhou, Debbie W. Leung, Isaac L. Chuang, Phys. Rev. A 62, 052316 (2000)