Quantum Information Processing (2022) 21:380
https://doi.org/10.1007/s11128-022-03732-1

Quantum multi-secret sharing via trap codes and discrete quantum walks

Shion Samadder Chaudhury[1] · **Sabyasachi Dutta**[2]

Received: 5 April 2022 / Accepted: 3 November 2022 / Published online: 14 November 2022

Abstract

In this paper, we propose a *fully quantum multi-secret sharing scheme*. In contrast with regular secret sharing schemes, multi-secret sharing schemes share a set of unknown secrets, and during the reconstruction phase, all the secrets are reconstructed. The main technique is to suitably modify a *quantum trap code* to construct a scheme where increasing number of secret states are recovered as more and more participants combine their shares. It is desirable that the dimensions of the share states are within implementable limits. In view of this and due to the significantly large dimension of the share states produced by our first construction, we introduce a discrete-time quantum walk-based technique to reduce the dimension of the shares making the schemes more suitable for practical purposes. Our methods are unconditional and do not depend on any computational hardness assumptions like lattice-based problems. Our scheme is simple, secure against adversarial attacks and can be easily modified into several variants of multi-secret sharing schemes.

Keywords Quantum multi-secret · Discrete-time quantum walk · Random permutations · Trap code

Mathematics Subject Classification 94A60 · 81P94 · 94A62 · 81P73

List of symbols

$\mathbb{N}, \mathbb{Z}, \mathbb{C}$	Natural numbers, integers, complex numbers
$\mathcal{P}, p_i$	Set of participants, i-th participant

✉ Shion Samadder Chaudhury
chaudhury.shion@gmail.com

Sabyasachi Dutta
saby.math@gmail.com

[1] Translational Research in Mathematics, TCG Centres for Research and Education in Science and Technology, Salt Lake Sector V, Kolkata, West Bengal 700091, India

[2] Department of Computer Science, University of Calgary, University Dr NW, Calgary, AB T2N 1N4, Canada

$\Gamma, \Gamma_{YES}, \Gamma_{NO}$	Access structure, qualified sets, forbidden sets
(n, k)	k-out-of-n threshold access structure
t_i	i-th threshold
$S, \mathcal{S}$	Domain of secrets
$(SHARE, RECON)$	Secret sharing scheme
$\Pi_i^{(s)}$	Distribution on share of i-th participant
$I, X, \sigma_x, Y, Z, \sigma_z$	Pauli matrices
$\mathbb{P}_n$	Set of n-qubit Pauli matrices
$[n]$	$\{1, 2, \ldots, n\}$
$\sigma, \sigma_{n_i}, \sigma_{k_i}$	Permutation map (not to be confused with the Pauli operators)
$\|\phi\rangle$	Qubit/quantum state/secret
$Sh_{Th}(n, k), Rec_{Th}(n, k)$	Fully quantum threshold secret sharing scheme
$Share_{k,n}, Rec_{k,n}$	Semi-quantum threshold secret sharing scheme
U, R, C, S, F, G	Unitary operators
E_{ij}	Elementary matrix
$[C_1, \ldots, C_d]$	Block diagonal matrix

Abbreviations

SSS	Secret sharing scheme
MSSS	Multi-secret sharing scheme
QSSS	Quantum secret sharing scheme
QMSSS	Quantum multi-secret sharing scheme
QECC	Quantum error-correcting code

1 Introduction

Protection of sensitive data is one of the main goals of cryptography, and to this end, *secret sharing* is one of the most important cryptographic primitives which has been widely studied. Secret sharing (SS) was introduced independently by Shamir [1] and Blakely [2]. A secret sharing scheme (SSS) consists of a secret to be shared among a set of participants with the stipulation that when some predetermined subsets of participants called *qualified sets* pool their information together, they can reconstruct their secret. Also, some specified subsets of participants called *forbidden sets* should not have any information about the secret.

Several real-life scenarios demand more flexible or general SSSs, and this necessity has given rise to the extensive study of several variants of SSSs. One such necessity is for a SSS to be able to share multiple secrets at one go. Such SSSs are called *multi-secret sharing schemes*(MSSS) [3–7]. SSSs are often model dependant. But generally what is done is that in a MSSS, several secrets are distributed among a group of participants by a dealer and depending on the model of reconstruction, several MSSSs have been proposed. In one such model, only authorized sets can reconstruct the all the secrets by combining their shares (or their pseudo shares), while other subsets cannot know any information about them. In another model, the stipulation is that as more and participants combine their shares, they can recover more number of secrets from the

set of secrets which was originally shared. Such a variant is called a *multi-threshold* MSSS [8–13]. In another variant which is prevalent in the area of visual secret sharing, as more and more participants combine their shares, they get closer to a secret(this includes a predefined notion of closeness). This variant is named *progressive* secret sharing [14–16].

Related work With the advent of quantum computation, a natural extension of the above is to study quantum secret sharing (QSS) where the goal is to share and protect sensitive data in a quantum environment. QSS has been in extensively studied [17–24] The motivation to study QSS schemes(single secret) is twofold: (1) Semi-quantum: to share a classical secret in a quantum environment and (2) fully quantum: to share a quantum secret in a quantum environment. It has been pointed out by the authors in [20] that sharing a quantum state is more difficult than sharing classical information and hence fully quantum schemes are far lesser in number than semi-quantum ones. We have observed the same for quantum multi-secret sharing schemes(QMSSS) [25], and to the best of our knowledge, a QMSSS sharing quantum states has not been studied before. QMSSSs have found application in block-chains [26, 27] and in multiparty communication (secret sharing) [28–31]. We have also observed that in several MSSSs in the literature [13], the security is conditional and is based on the security of computationally hard problems like lattice-based problems. Construction of QSSSs using quantum walks has been studied recently in [32, 33]. The authors in [32] used quantum walks on a $4 \times d$ lattice folded into a torus and the Fourier coin to realize an entanglement-free QSS where the participants use a d-level state. In [33], the authors have utilized the additive properties of circular quantum walks to construct a threshold QSSS to share a single classical secret in a quantum environment. We have used product states in our constructions and the use of product states to construct entanglement-free QSS both in the both in the traditional and the multiparty case has been considered in [34, 35]. As we have noted before that sharing a quantum state in a quantum environment is a more challenging issue, we attempt to construct a more general fully quantum MSSS. Our construction works for general graphs and not only specialized graphs like the circle. Discrete-time quantum walks [36, 37] have also found application in other areas of quantum computation as in [38–40]. An excellent source containing several properties of discrete quantum walks is [41]. Quantum walks on graphs have been further studied in [42–44]. In visual SSSs, the secret is an image and the dealer splits the image into n shares (noise-like shadows). During reconstruction, the secret image can be reconstructed by k authorized shadows, while less than k shares reconstruct nothing of the original image. The advantage of visual secret sharing is that the secret image can be reconstructed by superimposing the k shares and with no cryptographic computation. In the progressive variant [14, 15, 45] of such schemes, the more the number of shadows are superimposed, the clearer (or closer to the original secret image) the reconstructed image is. In other words, the more the number of participants combine their shares, the closer they get to the secret. This involves a precise mathematical notion of closeness or clarity which varies among different papers in the literature. It is natural to study visual secret sharing in the quantum context [46, 47].

Quantum walks Quantum walks are quantum analogues of classical random walks. Just as classical randomized algorithms use random walks, quantum walks have proved to

be beneficial to the design of quantum algorithms [48]. The evolution of a quantum walk in discrete time is specified by the product of two unitary operators: (1) a "coin flip" operator and (2) a conditional shift operator, which are applied repeatedly. So starting from an initial state, after a finite amount of time, there is a list of quantum states which are reachable from the initial state. This set of reachable states can be completely described by specifying the initial state, the coin flip operator and the shift operator(s).

Suppose we want to share a set of quantum secrets among participants. It is costly and poses implementation challenges to share each of the secrets to all the participants via quantum SSSs. However, if the set of secrets form a set of reachable states starting from an initial state, then it is enough to share the initial state, the coin flip operator and the conditional shift operators, and in one shot, we can share the whole set of quantum secrets among participants in a quantum environment. This is the idea that we explore and develop in this paper.

Another question that we address in this paper is the following: *How to design the most general and practical quantum SSS?* For a secret sharing scheme to be practical, it is desirable that the scheme can accommodate as many participants as possible (possibly infinite) without refreshing the system periodically or without communicating with the old participants from time to time. Such quantum schemes have been considered in [49, 50] and are called *quantum evolving secret sharing schemes.* Now if we use these schemes in conjunction with a multi-secret sharing scheme whose set of secrets is the set of the reachable states from a quantum walk, then we can have a truly general quantum secret sharing which can share arbitrarily many secrets among unbounded number of participants. This is possible because quantum walks can be performed on infinite lattices for as long as possible.

Our contributions Our main contributions are as follows:

- First we construct an unconditional fully quantum MSSS—sharing a set of quantum states in a quantum environment utilizing a modification of the trap code [51, 52] to incorporate a incremental or multi-threshold properties.
- Since the use of trap code causes a blow up in the dimension of the shares, in the following sections, we attempt to reduce the dimensions of the share states utilizing discrete-time quantum walks and remove the use of trap codes.
- As applications, we construct multi-threshold variants of the quantum walk-based schemes which also do not use trap codes. We also show that our constructions can be used in the "progressive" setting where participants get *closer* to the secret as more and more participants combine their shares.
- Our construction is entanglement-free which makes practical implementation easier and can be potentially applied on a larger number of participants as compared to schemes utilizing entanglement. While the results of this paper are theoretical and the paper has an algorithmic flavour, the flexibility and scalability of our constructions and the significant reduction in the dimension of the share states to make the constructed schemes within the reach of practical implementation should appeal to physicists and practitioners as well. To the best of the knowledge of the authors, the technique of modifying the trap code, application of our technique in the quan-

tum progressive model and the use of discrete quantum walks in multi-threshold case have not been considered before.

Paper organization The paper is organized as follows. Section 2 describes the required tools and we give formal definitions of computational security of a QMSSS. In Sect. 3, we elaborate the construction of our QMSSS based on a modification of the trap code(see Sect. 3.1.1). In the next Sect. 4 we use quantum walks to construct variants of QMSSSs. The following Sect. 5 discusses generalizations to general access structures, outlines a model for a possible quantum progressive SSS and this followed by Sect. 6 where we discuss the security of our scheme against adversarial attacks. In Sect. 7, we compare our constructed scheme with the existing ones and study its advantages. In Sect. 8 we discuss some aspects and further applications of our scheme and we conclude the paper in Sect. 9.

2 Preliminaries

Definition 1 (*Access structure*) Let $\mathcal{P} = \{p_1, \ldots, p_n\}$ be a set of participants. A collection $\Gamma \subseteq 2^{\mathcal{P}}$ is *monotone* if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An *access structure* over $\mathcal{P}$, $\Gamma = (\Gamma_{YES}, \Gamma_{NO})$ is a pair of collections of sets $\Gamma_{YES}, \Gamma_{NO} \subseteq 2^{\mathcal{P}}$, such that Γ_{YES} and $2^{\mathcal{P}} \backslash \Gamma_{NO}$ are monotone, and $\Gamma_{YES} \cap \Gamma_{NO} = \phi$. Sets in Γ_{YES} are called *qualified*, and sets in Γ_{NO} are called *forbidden* sets.

Definition 2 (*Threshold access structures*) Let $1 \leq k \leq n$. A k-out-of-n or (n, k) threshold access structure Γ over a set of participants $\mathcal{P} = \{p_1, \ldots, p_n\}$ is the complete access structure accepting all subsets of size at least k, that is, $\Gamma_{YES} = \{A \subseteq \mathcal{P} : |A| \geq k\}$ and $\Gamma_{NO} = \{A \subseteq \mathcal{P} : |A| < k\}$.

Definition 3 (*Multi-threshold access structures*) A multi-threshold access structure consists of participants $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ and independent (t_i, n)-threshold access structures for $i = 1, 2, \ldots, m$ satisfying $t_1 < t_2 < \ldots < t_m$.

Definition 4 (*Secret sharing scheme (SSS)* [1, 2]) For an access structure and S ($|S| \geq 2$) a domain of secrets, an SSS $\mathcal{S}$ consists of a pair of algorithms $(SHARE; RECON)$ such that (i) $SHARE$ is a probabilistic sharing algorithm for generating shares of participants and (ii) $RECON$ is a deterministic reconstruction algorithm to recover the secret. $SHARE$ and $RECON$ satisfy the following conditions:

1. $SHARE$ on input a secret $s \in S$ outputs the shares $\{\Pi_1^{(s)}, \ldots, \Pi_n^{(s)}\})$ of the participants.
2. **Correctness** For every secret $s \in S$, every qualified subset in Γ_{YES} can reconstruct the secret. For $s \in S$, and $B \in \Gamma_{YES}$, it holds that

$$Pr[RECON(\{\Pi_i^{(s)}\}_{i \in B}, B) = s] = 1,$$

   where the probability is over the randomness of the sharing procedure.
3. **Privacy** For every unqualified subset $B \notin \Gamma_{YES}$, and every two secrets s_1 and s_2 belonging to S, the distribution of the secret shares of parties in B generated with

secret s_1 and the distribution of the shares of parties in B generated with secret s_2 are identical. Namely, the distributions $(\{\Pi_i^{(s_1)}\}_{i\in B})$ and $(\{\Pi_i^{(s_1)}\}_{i\in B})$ are identical.

Multi-secret sharing scheme (MSSS) A SSS where instead of a single secret, a set of secret is shared among participants. Let $S = \{s_1, \ldots, s_r\}$ be a set of secrets, where each s_i belonging to a set S_i, is shared among participants in such a way that each subset of $\mathcal{P}$ can recover a certain subset of S, but has absolutely no information on the remaining secrets. We follow the definition of Blundo et al. [3] in the following. For each subset of participants $A \subset \mathcal{P}$, we denote by $S_A \subset S$ the set of secrets that can be recovered by the participants in A, referred to as the A-secret-set. For monotone access structures, for any $A \subset B \subset \mathcal{P}$, it holds that $S_A \subset S_B$.

Definition 5 (*Multi-threshold multi-secret sharing scheme*) Given n participants, thresholds, $2 \leq t_1 < t_2 < \ldots < t_k \leq n$, and a set of secrets $\mathcal{S} = \{s_1, \ldots, s_r\}$, the following conditions are satisfied for a SSS to be multi-threshold and multi-SSS:

1. If the number of participants combining their shares is less than t_1, no information about any secret in $\mathcal{S}$ can be obtained. For any subset $A \subset \mathcal{P}$, participants have no information on any subset of secrets in $S \setminus S_A$.
2. Any subset $A \subset \mathcal{P}$ of participants can recover the A-secrets-set S_A. More precisely, for an increasing chain of subsets of secrets $S_{t_1} \subset S_{t_2} \subset \cdots \subset S_{t_k} = S$ indexed by the threshold values, a subset A of participants of size $t_i \leq |A| < t_{i+1}$ can recover the secrets of S_{t_i}. If the number of participants combining their shares is greater or equal to t_k, all secrets in $\mathcal{S}$ can be reconstructed.

Definition 6 (*Pauli matrices*) Single qubit Pauli matrices are

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X(=\sigma_x) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z(=\sigma_z) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$\text{and } Y = iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

An n-qubit Pauli matrix is given by the n-fold tensor product of single-qubit Paulis. The set of all n-qubit Pauli matrices is denoted by $\mathbb{P}_n$, where $|\mathbb{P}_n| = 4^n$.

Definition 7 (*Quantum one-time pad* [37]) n the Quantum one-time pad cryptosystem, we have

- an n-qubit string $|\xi\rangle = |\xi_1\rangle \ldots |\xi_n\rangle$,
- shared key: two n-bit strings k, k'.
- To encode qubit by qubit: $|\phi_i\rangle = \sigma_x^{k_i} \sigma_z^{k'_i} |\xi_i\rangle$.
- To decode qubit by qubit: $|\xi_i\rangle = \sigma_z^{k'_i} \sigma_x^{k_i} |\phi_i\rangle$.

Here, $|x_i\rangle$, $|\phi_i\rangle$ are qubits and σ_x and σ_z are Pauli matrices. When a quantum one-time pad is applied, to a party that does not know the key, the encoded text seems completely mixed (information theoretically) [53].

Definition 8 (*Permutation map*) A permutation map is a unitary operation that acts on n qubits and permutes the order of the qubits or equivalently permutes the indices of the qubits. A permutation σ on n qubits takes the i-th qubit to the $\sigma(i)$-th qubit.

Definition 9 (*Trap code* [51, 52]) In a trap code, we have

1. Encoding qubit by qubit

- apply a $[[n, 1, d]]$ quantum error-correcting code Enc which will correct up to t errors. (here $d = 2t + 1$).
- to the resulting, append n-qubit traps, first in the state $|0\rangle \langle 0|^{\otimes n}$ (X-traps) and second in the state half $|+\rangle \langle +|^{\otimes n}$ (Z-traps),
- permute the resultant $3n$ qubits by a random permutation σ, according to the key k_1.
- finally apply a Pauli encryption using the classical randomness in the key k_2.
- Mathematically, the encoding of a state ρ is denoted as

$$P_{k_2}\sigma_{k_1}(Enc(\rho) \otimes |0\rangle \langle 0|^{\otimes n} \otimes |+\rangle \langle +|^{\otimes n})\sigma_{k_1}^{\dagger} P_{k_2},$$

where corresponding to the two part secret key, $k = (k_1, k_2)$, σ_{k_1} is the k_1-th permutation, P_{k_2} is the k_2-th Pauli matrix.

2. Decoding

- Apply the inverse Pauli according to key k_2.
- to the resulting apply the inverse permutation σ^{-1} according to the key k_1.
- measure X-traps in the computational basis and the Z-traps in the Hadamard basis. If they are not in their original state, it is rejected.
- decode the quantum error-correcting code Enc.

It is required that the quantum error-correcting code used here is a Calderback-Shor-Steane (CSS) code and a self-dual code implemented by a Clifford circuit.

Definition 10 (*Discrete-time quantum walk* [41]) Quantum walk is the quantum version of classical random walks. The evolution of a quantum walk in discrete time is specified by the product of two unitary operators: (1) a "coin flip" operator and (2) a conditional shift operator, which are applied repeatedly. There are three existing models of quantum walks which we describe briefly as follows: (The notations and definitions are taken from [41])

1. **Arc-reversal** [42, 44] Consider an undirected graph $G = (V, E)$ with $|V| = n$ and $|E| = m$. The state space is $\mathbb{C}^m$. Replace each edge of G with a pair of opposite arcs. The characteristic vectors $e_{u,v}$ of the directed arcs (u, v) span $\mathbb{C}^m$. The coin flip map is given by the permutation matrix R that reverses each arc, i.e. $Re_{u,v} = e_{v,u}$. For any vertex u, let there be an order defined on its neighbours $f_u : \{1, 2, \ldots, \deg(u)\} \longrightarrow \{v, v \text{ is adjacent to } u\}$. Denote by $f_u(j)$ and $(u, f_u(j))$ the j-th neighbour and the j-th arc of u, respectively. Let C_u be a $\deg(u) \times \deg(u)$ matrix which sends $(u, f_u(j))$ to a superposition of the all the outgoing arcs of u and satisfying $C_u e_j = \sum_{k=1}^{\deg(u)} (e_k^T C_u e_j) e_k$. The quantum coin is given by the block diagonal matrix $C = [C_1, C_2, \ldots, C_n]$ with C_i forming the diagonal blocks. Hence, for each iteration, the transition matrix is given by $U = RC$, combination of a quantum coin and an arc flip. Common choices for quantum coins are the Fourier coin $F = (\frac{1}{\sqrt{d}} e^{2jk\pi i/d})_{jk}$ and the Grover coin $G = \frac{2}{d} J - I$.

2. **Shunt-decomposition** [43] In this case, the graphs are assumed to be d-regular. Hence, the state space $\mathbb{C}^m$ is isomorphic to $\mathbb{C}^n \otimes \mathbb{C}^d$. The arc $(u, f_u(j))$ can be represented by $e_u \otimes e_j$. The transition matrix is $U = SC$, where C is a quantum coin as before and for each vertex, S maps its j-th arc to the jth arc of $f_u(j)$. S is a $0-1$ permutation matrix which is equivalent to the block diagonal matrix

$$S = \begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_d \end{pmatrix},$$

where P_j maps a vertex to its j-th neighbour. U has the following decomposition:

$$U = (P_1 \otimes E_{11} + \ldots + P_d \otimes E_{dd})(E_{11} \otimes C_1 + \ldots + E_{dd} \otimes C_n),$$

where E_{ij} is an elementary matrix with 1 in the ij-th entry and 0 elsewhere.

3. **Two-reflections** [38, 39] Let M be a Markov chain on G. let N denote the matrix obtained from M by taking the square root of its entries. Define

$$Q_1 = (e_1 \otimes (Ne_1) \ldots e_n \otimes (Ne_n))$$

and

$$Q_2 = ((N^T e_1) \otimes e_1 \ldots (N^T e_n) \otimes e_n).$$

Since M is doubly stochastic, we have $Q_1^T Q_1 = Q_2^T Q_2 = I$. Finally, U is defined as

$$U = R_1 R_2 = (2Q_1 Q_1^T - I)(2Q_2 Q_2^T - I).$$

Effectively, Q_1 partitions the arcs according to their tails, and Q_2 partitions the arcs according to their heads.

3 Technical details

Deviating from traditional SSSs for single secrets s, our aim is to share a subset of secrets $\mathcal{S}_r \subset S$ where the set of secrets is a finite set of quantum states $\mathcal{S} = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_u\rangle\}$. We assume existence of quantum threshold SSS (both fully quantum [20] and semi-quantum [21] models) which we need for our constructions. In our constructed scheme, there is a minimum threshold t_1. If the number of participants cross this threshold, they can reconstruct a certain minimum number of secret states but not the whole set of secrets. More number of participants are required to reconstruct more number of secret state. Finally, there is a maximum threshold and if the number of participants cross this threshold, they can reconstruct the full set of secrets. For

concrete definition, we refer to Definition 5 suitably adjusted to the case of quantum secrets. For the ease of reference, we introduce the following terms.
Incremental thresholds $1 < t_1 < t_2 < \ldots < t_k < n$, where n is the total number of participants and t_i's are thresholds.
Fully qualified sets A set is fully qualified if the number of participants combining their shares p satisfies $p \geq t_k$.
Semi-qualified sets A set is semi-qualified if the number of participants combining their shares p satisfies $t_1 \leq p < t_k$.
Forbidden sets A set is forbidden if the number of participants combining their shares p satisfies $p < t_1$.
One may interpret the above conditions to be reminiscent of a ramp scheme. In a ramp SSS qualified sets can reconstruct the secret and forbidden sets have no information about the secret. There is a third class of subsets of participants called semi-qualified who have partial information about the secret. In the present context, we have chosen not to call our scheme a ramp scheme due to the fact that semi-qualified sets can completely recover a predetermined chosen subset of the set of secrets. We have not considered or have made no attempt to quantify the information context of a subset of secrets. However, in the case of progressive secret sharing (see Sect. 5.3), one may call our scheme a ramp scheme as there is a well-defined notion of closeness to the original secret and as more and more participants combine their shares, they get closer to the secret.

3.1 Main scheme

In this section, we put forward our constructions. In Sect. 3.1.1, we detail our modification to the trap code. Next (Sect. 3.1.2) based on this modification, we present the construction of a fully quantum QMSSS with multiple-thresholds where there is no relation between the secret quantum states. We describe in detail the correctness and privacy of our scheme in Sect. 3.2 and analyse the dimension of the shares states in Sect. 3.3.

3.1.1 Modification to the trap code

As we have mentioned before, our construction is based on a modification to the trap code. The modification is done as follows: Recall Definition 10 where mathematically the encoding of a state ρ is given by $P_{k_2}\sigma_{k_1}(Enc(\rho) \otimes |0\rangle\langle 0|^{\otimes n} \otimes |+\rangle\langle +|^{\otimes n})\sigma_{k_1}^{\dagger} P_{k_2}$. By removing the Pauli operator, the state becomes $\sigma_{k_1}(Enc(\rho) \otimes |0\rangle\langle 0|^{\otimes n} \otimes |+\rangle\langle +|^{\otimes n})\sigma_{k_1}^{\dagger}$. Consider the permutation σ without the index. Assume that σ has no fixed points, i.e. σ is a derangement and has the following form. Suppose $\sigma : [n] \longrightarrow [n]$. Consider a partition of $[n]$ as $[n] = n_1 \cup n_2 \cup \ldots \cup n_r$. Let $\sigma_{n_i} : [n] \longrightarrow [n]$ such that $\sigma_{n_i}(j) = j$ for each $j \in [n] \backslash n_i$ and $\sigma_{n_i}(j) \neq j$ for each $j \in n_i$, $1 \leq i \leq r$. Suppose

$$\sigma = \underset{1 \leq i \leq r}{\circ} \sigma_{n_i} = \sigma_{n_1} \circ \ldots \circ \sigma_{n_r}.$$

In the original trap code, σ is chosen from all permutations of length n and the total number of choices is $n!$. In our case, we shall choose σ from all derangements of length $|n_i|$, $1 \leq i \leq r$. It is well known that the total number of derangements of length $|n_i|$ equals $|n_i| \sum_{k=0}^{|n_i|} \frac{(-1)^k}{k!}$. Hence, the total number choices for σ becomes

$$\prod_{i=1}^{r} \left(|n_i| \sum_{k=0}^{|n_i|} \frac{(-1)^k}{k!} \right).$$

This choice does not affect privacy as the permutations are chosen uniformly at random. The advantage of such a decomposition is that one can share the indices of the smaller permutations in an incremental manner through a multi-threshold SSS. The effect is that as more and more participants combine their shares, more partitions of the permutation can be unpermuted and hence more number of secrets can be reconstructed. This is formalized in step 7 of procedure 1. It was noted in [51, 52] that the same permutation should be applied on all the input qubits. Note that, same permutations are used on each partition, and fresh keys for the quantum one-time pad (Pauli) are used, hence our modification does not hamper security.

Remark 1 This method of using a partitioned permutation is reminiscent of the two-level classical SSS of [54] where the share strings are partitioned into blocks and random permutations are applied on the smaller blocks. However, in our method, we partition the set of secrets instead of the shares. There is no attempt in [54] to reduce the share. In this paper, on the other hand, we are able to significantly reduce the dimension of the share states using quantum walks.

3.1.2 No relation between secret states

Let us suppose that we have an unknown set of quantum secrets $\mathcal{S} = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_u\rangle\}$. Based on a coin toss, an l-subset $\mathcal{S}_r = \{|\phi_{i_1}\rangle, |\phi_{i_2}\rangle, \ldots, |\phi_{i_l}\rangle\} \subseteq \mathcal{S}$ is chosen.
Basic components Consider an increasing chain of thresholds $t_1 < t_2 < \cdots < t_r$. We shall assume that $l \geq t_r$ otherwise by the pigeon hole principle, there must be thresholds t_i and t_{i+1} such that the number of secrets recovered by number of participants greater than t_i and t_{i+1} remain same and a threshold t_{i+1} becomes redundant. Let $(Sh_{Th}(n,k), Rec_{Th}(n,k))$ be a fully quantum perfect threshold SSS sharing a quantum state as in [20]. Let $(Share_{(t_i,n)}, Rec_{(t_i,n)})$ be semi-quantum perfect threshold SSSs sharing classical secrets for all i as in [21].

Procedure 1: Share Composite State SHARE1

1. $\mathcal{S}_r \longleftarrow \{|\phi_{i_1}\rangle, |\phi_{i_2}\rangle, \ldots, |\phi_{i_l}\rangle\}$.
2. *Partition* $\mathcal{S}_r$ *into* r *subsets* $\mathcal{S}_r^1, \mathcal{S}_r^2, \ldots, \mathcal{S}_r^r$.
3. *Do steps 4 to 8 for each* w, $1 \leq w \leq r$.
4. $\mathcal{S}_r^w \longleftarrow \{|\phi_{i_1}\rangle, |\phi_{i_2}\rangle, \ldots, |\phi_{i_{l_w}}\rangle\}$.
5. $\left|\mathcal{S}_{temp1}^w\right\rangle \longleftarrow |\phi_{i_1}\rangle \otimes |\phi_{i_2}\rangle \otimes \ldots \otimes |\phi_{i_{l_w}}\rangle$
6. $\left|\mathcal{S}_{temp2}^w\right\rangle \longleftarrow Enc(\left|\mathcal{S}_{temp1}^w\right\rangle) \otimes |0\rangle\langle 0|^{\otimes l_w} \otimes |+\rangle\langle +|^{\otimes l_w}$.
7. $\left|\mathcal{S}_{comp1}^w\right\rangle \longleftarrow \sigma_{k_1}^w(\left|\mathcal{S}_{temp2}^w\right\rangle)\sigma_{k_1}^{w\dagger}$.
8. $|\mathcal{S}_{comp2}\rangle \longleftarrow \bigotimes_{1\leq w\leq r} \left|\mathcal{S}_{comp1}^w\right\rangle$
9. $|\mathcal{S}_{comp}\rangle \longleftarrow P_{k_2} |\mathcal{S}_{comp2}\rangle P_{k_2}$.
10. *Run* $Sh_{Th}(n, t_1)$ *on* $|\mathcal{S}_{comp}\rangle$ *to generate shares* $|Sh_1\rangle, |Sh_2\rangle, \ldots, |Sh_n\rangle$.
11. *Run* $Share_{(t_1,n)}$ *on* k_2 *to generate shares* $\left|Sh_1^{k_2}\right\rangle, \left|Sh_2^{k_2}\right\rangle, \ldots, \left|Sh_n^{k_2}\right\rangle$.
12. *Run* $Share_{(t_i,n)}$ *on* σ_{l_i} *for each* i *to generate shares* $\left|Sh_1^{l_i}\right\rangle, \left|Sh_2^{l_i}\right\rangle, \ldots, \left|Sh_n^{l_i}\right\rangle$.
13. STOP.

Procedure 2: Reconstruction RECON1

1. *Get shares* $|Sh_1\rangle, |Sh_2\rangle, \ldots, |Sh_k\rangle$.
2. *Run* $Rec_{Th}(n, t_1)$ *on* $|Sh_1\rangle, |Sh_2\rangle, \ldots, |Sh_k\rangle$ *to reconstruct* $|\mathcal{S}_{comp}\rangle$.
3. *Get shares* $\left|Sh_1^{k_2}\right\rangle, \left|Sh_2^{k_2}\right\rangle, \ldots, \left|Sh_k^{k_2}\right\rangle$.
4. *Run* $Rec_{(t_1,n)}$ *on* $\left|Sh_1^{k_2}\right\rangle, \left|Sh_2^{k_2}\right\rangle, \ldots, \left|Sh_k^{k_2}\right\rangle$ *to reconstruct* k_2.
5. *Get shares* $\left|Sh_1^{l_i}\right\rangle, \left|Sh_2^{l_i}\right\rangle, \ldots, \left|Sh_k^{l_i}\right\rangle$ *for each* i.
6. *Find* t_m *such that* $t_m \leq k < t_{m+1}$.
7. $Rec_{(t_i,n)}$ *on* $\left|Sh_1^{l_i}\right\rangle, \left|Sh_2^{l_i}\right\rangle, \ldots, \left|Sh_k^{l_i}\right\rangle$ *for* $i = 1, \ldots, m$ *such that* $t_m \leq k < t_{m+1}$*; and obtain* $\sigma_{l_0}, \ldots, \sigma_{l_m}$.
8. *On* $|\mathcal{S}_{comp}\rangle$
   - *use the key* k_2 *to remove the Pauli operator* P_{k_2} *to get* $|\mathcal{S}_{comp2}\rangle$,
   - *on* $|\mathcal{S}_{comp2}\rangle$ *use the decomposition* $|\mathcal{S}_{comp2}\rangle \longleftarrow \bigotimes_{1\leq w\leq r} \left|\mathcal{S}_{comp1}^w\right\rangle$,
   - *use* $\sigma_{l_1}, \ldots, \sigma_{l_m}$ *to invert the permutations on the first* m *subsets and obtain* $\left|\mathcal{S}_{temp2}^w\right\rangle$ *for* $w = 1, \ldots, m$.
9. *On* $\left|\mathcal{S}_{temp2}^w\right\rangle$ *discard the* $|0\rangle$ *and* $|1\rangle$ *states (traps) to get the state* $Enc(\left|\mathcal{S}_{temp1}^w\right\rangle)$.
10. *Decode the QECC to get the partially decoded states* $\left|S_{temp1}^w\right\rangle$*'s which use the tensor product of the original secret states.*
11. *Obtain the original states from the quantum lines.*
12. STOP.

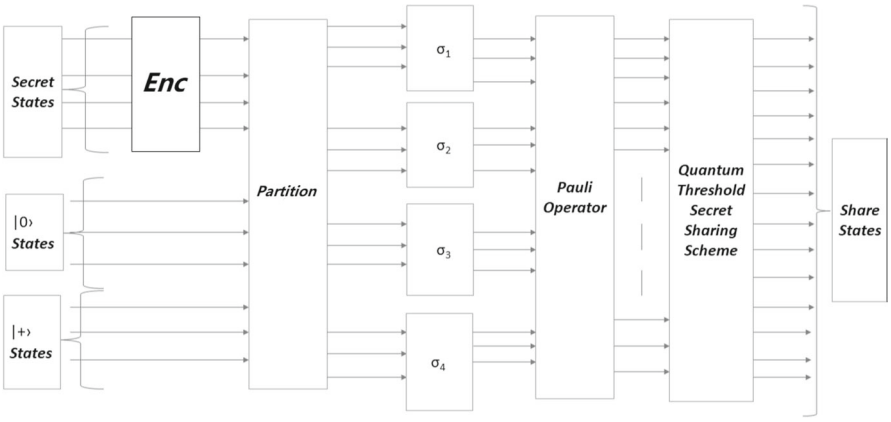

Fig. 1 Schematic diagram of QMSSS

In Fig. 1, we give a schematic diagram of our construction.

3.2 Correctness and privacy

The proof of correctness and security of the proposed scheme depend on the same properties of its basic building blocks. We first summarize/outline them and then move onto proving the correctness and security of our proposal.

Description of $(Sh_{Th}(n,k), Rec_{Th}(n,k))$ **of** [20]. Here, the secret is an unknown quantum state.

1. Distribution of shares via a polynomial computation: The dealer finds a suitable prime number d and sets a finite field $\mathbb{Z}_d$. Depending of the number of participants t who can recover the secret, the dealer randomly chooses $t-1$ elements $a_i \in \mathbb{Z}_d$ $(i = 1, ..., t-1)$. Next the dealer defines the polynomial $f(x) = S + a_1 x + \ldots + a_{t-1} x^{t-1}$, $S \in \mathbb{Z}_d$. For n participants, the dealer evaluates the polynomial on n different elements of $\mathbb{Z}_d$ and sends the outputs privately to each participant.
2. Suppose the dealer generates an unknown sequence of states to be shared among the participants. Next comes the application of a phase shift operation $R_z(\theta) = \cos\theta\,|0\rangle\langle 0| - \sin\theta\,|0\rangle\langle 1| + \sin\theta\,|1\rangle\langle 0| + \cos\theta\,|1\rangle\langle 1|$ on every quantum state in the unknown sequence of quantum states generated by the dealer, where $\theta = 2\pi - \frac{S}{N}$, N being the security coefficient.
3. Insertion of random decoy particles $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ for eavesdropping detection.

All the steps mentioned above are part of the secret sharing procedure in [20]. The corresponding secret recovery procedure consists of the application of the corresponding Lagrange's interpolation and application of proper phase shift operations. The details are omitted.

Description of $(Share_{(n,k)}, Rec_{(n,k)})$ **of** [21]. Here, the secret is a classical secret $S \in \mathbb{Z}_d$. Next the dealer defines the polynomial $f(x) = S + a_1 x + \ldots + a_{t-1} x^{t-1}$, $S \in \mathbb{Z}_d$ as before. For n participants, the dealer evaluates the polynomial on n different

elements x_i of $\mathbb{Z}_d$ and satisfies each $L_i = \prod_{1 \leq j \leq n, j \neq i} \frac{x_j}{x_j - x_i}$ is an integer and shares the outputs privately to each participant. During reconstruction, the dealer generates a two-qudit Bell state in the d-dimensional Hilbert space. The participants perform suitable unitary operations on this Bell state to reconstruct the secret. For more details, we refer the reader to [21].

Encoding of U See Sect. 4.4.3.

3.2.1 Description of procedures 1 and 2 and correctness of the scheme

Figure 1 gives a schematic diagram of our construction.

Procedure 1 **SHARE1** Procedure 1 first chooses a subset $\mathcal{S}_r$ of the set of secrets $\mathcal{S}$. In step 2, this chosen subset is then partitioned into r partitions. For each partition, temporary composite states are created. This is done by taking the tensor product of the quantum states present in a partition. To the obtained state, the trap code operations are applied, i.e. a suitable quantum error-correcting code is applied, equal number of $|0\rangle$ and $|+\rangle$ states are appended followed by a random permutation and the application of a random Pauli operator. Thus, from each partition, we obtain a composite state which looks completely mixed due to the application of the trap code. Finally, all the composite states from each of partitions are combined (tensored) to get the state $\left|\mathcal{S}_{comp}\right\rangle$. To this state, the underlying quantum threshold secret scheme is applied to get the shares of the participants. Additionally, the index k_2 of the k_2 Pauli operator is shared via an underlying semi-quantum threshold SSS. Similarly, the index of the random permutation for each of the partition has to be shared. This is again done by applying a semi-quantum threshold SSS.

Procedure 2 **RECON1** Let us suppose that some k participants present their shares. If $k \geq t_0$, then by applying the reconstruction procedure of the underlying quantum threshold SSS, the state $\left|\mathcal{S}_{comp}\right\rangle$ is recovered. Similarly, by applying the reconstruction procedure of the underlying quantum threshold schemes, the index of the Pauli operator is recovered. Next, the greatest threshold t_m which is less than k is identified. From step 7, the indices of the respective permutations which were applied to the first m permutations are recovered. The random permutations are inverted, the trap states ($|0\rangle$ and $|1\rangle$ states are discarded), the QECC is decoded and hence, the secret quantum states which belong to the first m partitions are recovered.

Theorem 1 *The constructed scheme is correct. Fully qualified sets can recover all the states in* $\mathcal{S}_r$. *If* $p_1 < t_m \leq p_2$, *then the number of states recovered by* p_1 *participants is strictly less than the number of states recovered by* p_2 *participants.*

Proof A fully qualified set contains more than t_r number of participants. By the correctness of the underlying threshold schemes, the state $\left|\mathcal{S}_{comp}\right\rangle$ can be recovered and also the index of the applied Pauli operator k_2 can be identified to remove it from the recovered $\left|\mathcal{S}_{comp}\right\rangle$ to get the state $\left|\mathcal{S}_{comp2}\right\rangle$. Since the number of participants satisfies all the thresholds, again by the correctness of the underlying threshold SSSs, all the indices of the permutations are recovered. The permutations are inverted, the applied error correcting code is decoded, and the original quantum states are obtained from the respective quantum lines. Note that, the number of partitions/states on which the

applied permutation can be inverted depends on the number of thresholds the participants satisfy. Hence, suppose the maximum threshold satisfied is t_m, then only the first m permutations can be unpermuted and finally recovered. Thus, we can conclude the second part of the theorem. □

3.2.2 Privacy

Theorem 2 *Forbidden sets cannot reconstruct any secret state. Any subset of participants which is not qualified cannot reconstruct the full set of secrets. The number of secret states reconstructed increases as the number of participants crosses the given thresholds.*

Proof Let us suppose that a forbidden set presents its shares. By the privacy of the underlying threshold SSSs, the recovered state is independent from $\left|\mathcal{S}_{comp}\right\rangle$. Also, the recovered index of the permutations and the index of the Pauli operator are independent of the actual indices. Since these are independent events, one can conclude that the joint distributions for two different r-sets of quantum states $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathcal{S}$, $(\{\Pi_r^{(\mathcal{S}_1)}\}_{r\leq|\mathcal{S}|})$ and $(\{\Pi_r^{(\mathcal{S}_2)}\}_{r\leq|\mathcal{S}|})$ are identical. Also, note that in contrast to trap codes where the probability is computed over all permutations of some length N(to be specified later), in our case, the probability is computed over all such permutations of length N which can be expressed as a product of r permutations(one for each partition). Clearly, if the maximum threshold satisfied is $t_m(m < r)$, then the permutations corresponding to the partitions($> m$) cannot be unpermuted. And hence not all states can be recovered. □

3.3 Dimension of share states

We shall assume for ease of computation that the underlying quantum threshold SSS $(Sh_{Th}(n,k), Rec_{Th}(n,k))$ does not increase the dimension of the share state. We also note that applying a quantum one-time pad does not change the dimension of the state. In view of this, it is enough to compute the dimension of $\left|\mathcal{S}_{comp}\right\rangle$. Let the dimension of the states in $\mathcal{S}$ be bounded above by $D_{\mathcal{S}}$. Also, let the size of a partition be bounded above by P_r. Let μ be the factor by which the QECC increases the dimension of the state and suppose for each partition a maximum of M traps are applied. Hence, for each partition, the dimension of $\left|\mathcal{S}^w_{comp1}\right\rangle$ is bounded above by $K = D_{\mathcal{S}} \times P_r \times \mu \times M$. Hence, the total dimension of $\left|\mathcal{S}_{comp}\right\rangle$ is bounded above by $O(K^r)$.

Furthermore, quantum states corresponding to the Pauli operators and the random permutations are also shared. Even for a small number of states and/or partitions the dimension of the shares corresponding to $\left|\mathcal{S}_{comp}\right\rangle$ can become very large for practical applications. The blowup is also due to the QECC which increases dimension. This motivates us to consider techniques to significantly reduce the dimension of the share states which does not use trap codes. We describe the modifications in the following sections.

4 Modifications and variants

In this section, we attempt to reduce the dimension of the share states. The crucial assumption here is that there is a known relation between the secret quantum states. We show that this assumption helps to drastically reduce the dimension of the share states and also that the known relation between the secret states does not reveal any information about the states to the forbidden states. As a warm-up (Sect. 4.1), we present procedure 3 and 4, where the states are related by the powers of a single unitary operator. To model more general situations, we introduce our quantum walk-based constructions in Sect. 4.4.

4.1 Relation between quantum states described by a finite number of unitary operators

The main idea in this section is that to share a set of secrets with some known relations among the states, it is not necessary to share all the secret states. Again let us suppose that we have an unknown set of quantum secrets $\mathcal{S} = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_u\rangle\}$. In addition, let us suppose that $|\phi_i\rangle = U^{i-1}(|\phi_1\rangle)$ for all $i = 0, 1, \ldots, n$. In this case, it is enough to share $|\phi_1\rangle$, the number of quantum states n and an encoding of the operator U. Hence, in Procedure 3, we essentially reduce the MSS problem to the case of sharing just three secrets, one quantum secret and two classical secrets in the quantum environment. However, situations need not be so simple and might demand complicated relations between known states. In view of this, we generalize the this method to more complicated scenarios using the concept of discrete-time quantum walks in Sect. 4.4.

Procedure 3: Share composite state SHARE2

1. $\mathcal{S}_r \longleftarrow |\phi_1\rangle$.
2. *Run* $Sh_{Th}(n,k)$ *on* $|\mathcal{S}_r\rangle$ *to generate shares* $\left|Sh_1^{\phi}\right\rangle, \left|Sh_2^{\phi}\right\rangle, \ldots, \left|Sh_n^{\phi}\right\rangle$.
3. $\mathcal{S}_2 \longleftarrow m$
4. *Run* $Share^1_{(n,k)}$ *on* $\mathcal{S}_2$ *to generate shares* $\left|Sh_1^{m}\right\rangle, \left|Sh_2^{m}\right\rangle, \ldots, \left|Sh_n^{m}\right\rangle$.
5. $\mathcal{S}_3 \longleftarrow$ *an encoding of* U.
6. *Run* $Share^2_{(n,k)}$ *on* $\mathcal{S}_3$ *to generate shares* $\left|Sh_1^{U}\right\rangle, \left|Sh_2^{U}\right\rangle, \ldots, \left|Sh_n^{U}\right\rangle$.
7. $\left|Sh_i^{\phi}\right\rangle, \left|Sh_i^{m}\right\rangle, \left|Sh_i^{U}\right\rangle \longleftarrow$ *Share of participant* P_i.
8. STOP.

Procedure 4: Reconstruction RECON2

1. *Get shares* $(\left|Sh_1^{\phi}\right\rangle, \left|Sh_1^{m}\right\rangle, \left|Sh_1^{U}\right\rangle), \ldots, (\left|Sh_k^{\phi}\right\rangle, \left|Sh_k^{m}\right\rangle, \left|Sh_k^{U}\right\rangle)$.
2. *Run* $Rec_{Th}(n,k)$ *on* $\left|Sh_1^{\phi}\right\rangle, \left|Sh_2^{\phi}\right\rangle, \ldots, \left|Sh_k^{\phi}\right\rangle$ *to get* $|\phi_1\rangle$.
3. *Run* $Rec^1_{(n,k)}$ *on* $\left|Sh_1^{m}\right\rangle, \left|Sh_2^{m}\right\rangle, \ldots, \left|Sh_k^{m}\right\rangle$ *to get* m.
4. *Run* $Rec^2_{(n,k)}$ *on* $\left|Sh_1^{U}\right\rangle, \left|Sh_2^{U}\right\rangle, \ldots, \left|Sh_k^{U}\right\rangle$ *to get* U.
5. *Compute* $U(|\phi_1\rangle), U^2(|\phi_1\rangle), \ldots, U^{m-1}(|\phi_1\rangle)$ *to get the states* $|\phi_2\rangle, |\phi_3\rangle, \ldots, |\phi_m\rangle$.
6. STOP.

4.2 Correctness and privacy

Theorem 3 *The constructed scheme is correct, i.e. any k or more participants performing the reconstruction procedure by combining their shares can reconstruct all the secrets* $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, \ldots, |\phi_m\rangle$.

Proof From Procedure 3 (i.e. SHARE2), we observe that the initial secret state $|\phi_1\rangle$ is shared via an fully quantum (n, k) threshold SSS. The maximum power m to which U is raised and an encoding of U which are treated as classical secrets are shared using semi-quantum (n, k) threshold SSSs. Now from Procedure 4 (i.e. RECON2), we see that in order to reconstruct all the secrets, the respective reconstruction procedures are applied to recover $|\phi_1\rangle$, m and U. Finally, the participants compute $U(|\phi_1\rangle), U^2(|\phi_1\rangle), \ldots, U^{m-1}(|\phi_1\rangle)$ to get the states $|\phi_2\rangle, |\phi_3\rangle, \ldots, |\phi_m\rangle$. □

Theorem 4 (Privacy) *Forbidden sets of participants (i.e. subsets with size less than or equal to* $k-1$*) cannot reconstruct any secret state.*

Proof To reconstruct all the secret states in the state, it is necessary to reconstruct $|\phi_1\rangle$ and U. By the privacy of the underlying k-out-of-n quantum threshold SSSs, any forbidden set of participants (i.e. subsets containing $\leq k-1$ participants) cannot reconstruct either of $|\phi_1\rangle$ or U. Hence, forbidden sets of participants cannot reconstruct any secret state. The reconstruction of m is not entirely necessary as the participants can start computing $U^i(|\phi_1\rangle)$, and without the knowledge of m, the participants cannot claim with certainty that they have recovered all the quantum states. Hence, to exactly reconstruct all the secret quantum states, it is necessary to reconstruct all of $|\phi_1\rangle$, m and U which a forbidden set of participants cannot. □

4.3 Dimension of share states

Let $D_{\mathcal{S}}$ be the dimension of $|\phi_1\rangle$. Let us assume that application of the underlying quantum threshold SSS $(Sh_{Th}(n, k), Rec_{Th}(n, k))$ does not increase the dimension of the share state. Also, the semi-quantum threshold schemes share classical secret privately to the participants and utilize a d-dimensional state for secret reconstruction. In view of this, one can assume a constant times increase in the overall dimension of the share states. Assuming for ease of computation that the dimension of the share state due to sharing m is bounded above by $D_{\mathcal{S}}$, the dimension of a share state is bounded above by $O(D_{\mathcal{S}}^2)$. In comparison with the dimension obtained in Sect. 3.3, we have $D_{\mathcal{S}}^2 \ll K^r$ and this is a significant improvement.

4.4 Quantum multi-secret sharing schemes based on quantum walks

We can express a QMSSS in terms of a *Discrete-Time Quantum Walk Model*. We shall construct three SSSs based on the three types of discrete-time quantum walks we have defined in Sect. 2.

4.4.1 Arc reversal model

In this model, we have the following components:

- A graph G where each edge is replaced by two directed edges(arcs) in the opposite direction. Let us suppose that X has n vertices and m arcs.
- State space is $\mathbb{C}^m$ spanned by the characteristic vector of the arcs $e_{u,v}$.
- For each vertex u, there is a linear order f_u on its neighbours.
- The transition matrix of an arc reversal quantum walk is given by $U = RC$ where R is a permutation matrix that reverses an arc and C is a coin flip quantum operator. We may give the same quantum coin C to all the vertices or we can give different quantum coins to different vertices.
- **A QMSSS based on the Arc reversal model** Let us suppose that we have a graph $G = (V, E)(E$ consists of arcs), an arc reversal operator R and each vertex has two quantum coins C_0 and C_1. Hence, we have two phase transition matrices $U_0 = RC_0$ and $U_1 = RC_1$. Let the characteristic vectors corresponding to the arcs be denoted by $e_{u,v}$. Fix an $N \in \mathbb{N}$. The set of secrets is defined as

$$\begin{aligned}\mathcal{S}_N = \{&A_1 \circ A_2 \circ \ldots \circ A_i(|\phi\rangle), 1 \leq i \leq \log N, A_i = U_0, U_1, |\phi\rangle \\ &= e_{u,v}, (u, v) \in E\}.\end{aligned}$$

To choose a multi-secret, we do the following procedure. Let $|\phi\rangle = e_{u,v}$ be a fixed initial state. For any $\mathcal{X} \leq N$, let us consider the binary expansion of $\mathcal{X}$ denoted as $(x_1, x_2, \ldots, x_{\log \mathcal{X}})_2$. Hence, $x_k = 0, 1(1 \leq k \leq \log \mathcal{X})$. Corresponding to $\mathcal{X}$, we can get a quantum multi-secret as follows: If $x_2 = 0$, then $|\phi_1\rangle = U_0(|\phi\rangle)$, otherwise $x_2 = 1$ and $|\phi_1\rangle = U_1(|\phi\rangle)$. Again if $x_3 = 0$, then $|\phi_2\rangle = U_0(|\phi_1\rangle)$, otherwise $x_3 = 1$ and $|\phi_2\rangle = U_1(|\phi_1\rangle)$ and this process is continued until we reach $\log \mathcal{X}$. Formally, the multi-secret is

$$\mathcal{S}_{\mathcal{X}} = \{A_1 \circ A_2 \circ \ldots \circ A_i(|\phi\rangle), 1 < i \leq \log \mathcal{X}, A_1 = I, A_i = U_{x_i}\}.$$

Hence, in this process, it is necessary to share the initial state ϕ, a natural number $\mathcal{X}$. The remaining components like the graph G, and the unitary operators U_1 and U_2 may remain public or private depending on the model being used or depending on the maximum dimension of the share states that is allowable by the implementing devices. The procedure is formalized in the following algorithms.

Procedure 5: Share composite state SHARE3

1. $\mathcal{S}_{initial} \longleftarrow |\phi_1\rangle$.
2. *Run* $Sh_{Th}(n,k)$ *on* $|\mathcal{S}_i\rangle$ *to generate shares* $\left|Sh_1^{\phi}\right\rangle, \left|Sh_2^{\phi}\right\rangle, \ldots, \left|Sh_n^{\phi}\right\rangle$. *(*$Sh_{Th}(n,k)$ *is the share procedure of a fully quantum threshold SSS)*
3. $\mathcal{S}_2 \longleftarrow$ *an encoding of* $\mathcal{X}$ *(*$\log \mathcal{X}$ *being the length of the random walk.)*
4. *Run* $Share^1_{(n,k)}$ *on* $\mathcal{S}_2$ *to generate shares* $\left|Sh_1^{x}\right\rangle, \left|Sh_2^{x}\right\rangle, \ldots, \left|Sh_n^{x}\right\rangle$. *(*$Share^1_{(n,k)}$ *is the share procedure of a semi-quantum threshold SSS)*
5. $\mathcal{S}_3 \longleftarrow$ *a classical encoding of* U_0.
6. *Run* $Share^2_{(n,k)}$ *on* $\mathcal{S}_2$ *to generate shares* $\left|Sh_1^{U_0}\right\rangle, \left|Sh_2^{U_0}\right\rangle, \ldots, \left|Sh_n^{U_0}\right\rangle$.
7. $\mathcal{S}_4 \longleftarrow$ *a classical encoding of* U_1.
8. *Run* $Share^3_{(n,k)}$ *on* $\mathcal{S}_4$ *to generate shares* $\left|Sh_1^{U_1}\right\rangle, \left|Sh_2^{U_1}\right\rangle, \ldots, \left|Sh_n^{U_1}\right\rangle$.
9. $\left|Sh_i^{\phi}\right\rangle, \left|Sh_i^{m}\right\rangle, \left|Sh_i^{U_0}\right\rangle, \left|Sh_i^{U_1}\right\rangle \longleftarrow$ *Share of participant* P_i.
10. *Share the graph* G.
11. STOP.

Note $(Sh_{Th}(n,k), Rec_{Th}(n,k))$ is a fully quantum SSS to share the initial state in a quantum environment. This is the same scheme as described in Sect. 3.2. Again we omit the exact details and refer the reader to [20]. $(Share^1_{(n,k)}, Rec^1_{(n,k)})$ is a semi-quantum threshold SSS to share the classical secret $\mathcal{X}$. We have briefly described this scheme in Sect. 3.2 in the discussion of $(Share_{(n,k)}, Rec_{(n,k)})$ of [21]. Similarly, $(Share^2_{(n,k)}, Rec^2_{(n,k)})$ and $(Share^3_{(n,k)}, Rec^3_{(n,k)})$ are semi-quantum threshold schemes to share classical secrets in a quantum environment.

Procedure 6: Reconstruction RECON3

1. *Get shares* $(\left|Sh_1^{\phi}\right\rangle, \left|Sh_1^{m}\right\rangle, \left|Sh_1^{U_0}\right\rangle, \left|Sh_1^{U_1}\right\rangle), \ldots, (\left|Sh_k^{\phi}\right\rangle, \left|Sh_k^{m}\right\rangle, \left|Sh_k^{U_0}\right\rangle, \left|Sh_k^{U_1}\right\rangle)$.
2. *Run* $Rec_{Th}(n,k)$ *on* $\left|Sh_1^{\phi}\right\rangle, \left|Sh_2^{\phi}\right\rangle, \ldots, \left|Sh_k^{\phi}\right\rangle$ *to get* $|\phi_1\rangle$.
3. *Run* $Rec^1_{(n,k)}$ *on* $\left|Sh_1^{x}\right\rangle, \left|Sh_2^{x}\right\rangle, \ldots, \left|Sh_k^{x}\right\rangle$ *to get* $\mathcal{X}$.
4. *Run* $Rec^2_{(n,k)}$ *on* $\left|Sh_1^{U_0}\right\rangle, \left|Sh_2^{U_0}\right\rangle, \ldots, \left|Sh_k^{U_0}\right\rangle$ *to get* U_0.
5. *Run* $Rec^3_{(n,k)}$ *on* $\left|Sh_1^{U_1}\right\rangle, \left|Sh_2^{U_1}\right\rangle, \ldots, \left|Sh_k^{U_1}\right\rangle$ *to get* U_1.
6. *Recover the graph* G
7. *Consider the binary expansion of* $\mathcal{X} = (x_1, x_2, \ldots, x_{\log \mathcal{X}})_2$
8. *Do steps 8 to 10 for* $i = 2$ *to* $\log \mathcal{X}$
9. *If* $x_i = 0$, *then* $|\phi_i\rangle = U_0(\left|\phi_{i-1}\right\rangle)$,
10. *If* $x_i = 1$, *then* $|\phi_i\rangle = U_1(\left|\phi_{i-1}\right\rangle)$
11. $i \longleftarrow i + 1$
12. *Return states* $|\phi_1\rangle, |\phi_2\rangle, \ldots, \left|\phi_{\log \mathcal{X}}\right\rangle$
13. STOP

4.4.2 Shunt decomposition model

The shunt decomposition model can be utilized in a similar manner as in the arc reversal model. This model is useful when the underlying graph has a certain symmetry. In this model, the graph G is assumed to be d-regular. Both in the classical and quantum

domain, special SSSs have been studied which can handle unbounded number of participants [49, 55]. We can similarly ask the following question: *what if the number of secrets to be shared is unbounded?* In this scenario, the shunt decomposition model becomes useful as this model has been applied to infinite paths and infinite grids. Here, also we have a coin operator C and a shift operator S and the transition matrix is given by $U = SC$. A QMSSS based on the shunt decomposition model can be easily constructed using procedures 5 and 6 by suitably modifying the quantum coin operators and the shift matrix S. Due to this similarity, we omit the exact details.

4.4.3 Two-reflections model

In this model, there is no quantum coin. The transition matrix is given by $U = (2Q_1Q_1^T - I)(2Q_2Q_2^T - I)$ where Q_1 and Q_2 represent two partitions of the underlying graph G, one based on the head of the arcs and the other based on the tails of the arcs [41]. As has been noted in [41, 56], these partitions can come from different graph structures, e.g. orientable embeddings. The important observation is that to share the operator U, it is enough the share the doubly stochastic matrix M and the partition of the arcs as classical secrets to be protected in a quantum environment via the semi-quantum threshold SSS $(Share_{(n,k)}, Rec_{(n,k)})$. One may use this U directly in Sect. 4.1.

4.5 Correctness and privacy

We first describe the share generation and reconstruction algorithms and then proceed to argue correctness and privacy of the scheme.

Procedure 5: In the SHARE3 algorithm, the secrets are the initial state $|\phi_1\rangle$, the length of the random walk $\mathcal{X}$ and the transition operators U_1, U_2. The state $|\phi_1\rangle$ is shared by a fully quantum threshold SSS. To share X and the transitions operators U_1, U_2 (or their proper encodings), we use semi-quantum threshold SS.

Procedure 6: The RECON3 procedure consists of recovering $|\phi_1\rangle$, the length of the random walk $\mathcal{X}$ and the transition operators U_1, U_2 by applying the respective reconstruction procedures of the underlying quantum threshold schemes. To reconstruct the remaining secrets, one considers the binary expansion of $\mathcal{X} = (x_1, x_2, \ldots, x_{\log \mathcal{X}})_2$. If $x_2 = 0$, then $|\phi_2\rangle = U_0 |\phi_1\rangle$, otherwise $|\phi_2\rangle = U_1 |\phi_1\rangle$. Again if $x_3 = 0$, then $|\phi_3\rangle = U_0 |\phi_2\rangle$, otherwise $|\phi_3\rangle = U_1 |\phi_2\rangle$. This process is continued to finally recover all the states until $\left|\phi_{\log \mathcal{X}}\right\rangle$.

We now have the following theorem.

Theorem 5 *The constructed scheme satisfies the correctness property, i.e. k participants combining their share can reconstruct all the secrets* $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, \ldots, \left|\phi_{\log \mathcal{X}}\right\rangle$. *Also, the scheme satisfies privacy property, in particular, forbidden sets containing less than k of the participants cannot reconstruct any secret state.*

Proof The correctness property easily follows from the correctness of the underlying schemes viz. $(Sh_{Th}(n,k), Rec_{Th}(n,k))$, and $(Share^1_{(n,k)}, Rec^1_{(n,k)})$ and $(Share^3_{(n,k)}, Rec^3_{(n,k)})$. To reconstruct all the secret states in the state, it is necessary to reconstruct

$|\phi_1\rangle$, $\mathcal{X}$, U_0 and U_1. By the privacy of the underlying quantum threshold SSSs, any forbidden set of participants which contains less than k participants cannot reconstruct any of $|\phi_1\rangle$, $\mathcal{X}$, U_0 and U_1. Moreover, the semi-quantum threshold schemes use a variant of Shamir's polynomial-based secret sharing and, therefore, $k-1$ or less number of shares statistically hides the secrets, viz. U_0 and U_1. Hence, forbidden sets of participants cannot reconstruct any secret state. The reconstruction of $\mathcal{X}$ is necessary as the bit pattern of $\mathcal{X}$ determines the further secret states $|\phi_2\rangle, \ldots |\phi_{\log \mathcal{X}}\rangle$. Hence, to exactly reconstruct all the secret quantum states, it is necessary to reconstruct all of $|\phi_1\rangle$, $\mathcal{X}$, U_0 and U_1 which a forbidden set of participants cannot. □

4.6 On the dimension of share states and possibility of reduction

The analysis is similar as in Sect. 4.3. We have an exponential reduction from K^r. However, the dimension of share states is more as compared to Sect. 4.3 due to more information to be shared among participants. Note that, depending on the model, one can even make U_0, U_1 public and even then the forbidden states cannot reconstruct the set of secrets. Assuming for ease of computation that the dimensions of the states due to $|\phi_1\rangle$, $\mathcal{X}$, U_0 and U_1 are bounded by $D_{\mathcal{S}}$, then the over dimension of the share states becomes $D_{\mathcal{S}}^4$. Depending on the model, one may make the operators U_0 and U_1 public and in that the dimension becomes $D_{\mathcal{S}}^2$. From the above discussion, we conclude that the steps 2 and 4 of procedure 5 are necessary.

For the practicality of implementation of quantum SSSs, the lesser the dimension of the share states, the easier it is to implement the scheme. To reduce the dimension, one can consider the possibility of making some of the steps of procedure 5 optional. Another instance where the dimension can be reduced is if we consider an interactive model. In this case, the dealer retains $\mathcal{X}$ and shares $|\phi_1\rangle$, U_0 and U_1. The reconstruction procedure consists of $\log \mathcal{X}$ rounds of interaction. In every round of interaction, the dealer tells the participants one bit in the binary expansion of $\mathcal{X}$. If the value is 0, participants apply U_0 and if the value is 1, participants apply U_1.

4.7 Generality of the construction

We have considered multi-SSSs where the quantum states are related to each other and this results in a major reduction in the dimension of the states. It may appear that it makes our construction restrictive in nature. We point out that by making a small modification, our construction can be applied to the case where there is no known relation between the secret states and still it is possible to reduce the dimension of the share states. Using the shunt decomposition model, we show that it is possible. Let the graph be chosen to be the complete graph K_n. The coin operator S is equivalent to the block diagonal matrix

$$S = \begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_d \end{pmatrix}$$

The blocks are obtained from the linear orders defined for each vertices on the set of their neighbours. We randomize these orders and equivalently we choose random permutation matrices as the blocks in the matrix S. The final effect is that after one step of the random walk, the probability of going from one state to any of the other states is equal. Hence, we can treat this case as sharing multiple secret states which have no relation between them since the states are reached with equal probability.

5 Generalization and applications

5.1 General access structures

Our schemes use threshold quantum SSSs as basic building blocks, and as a result, they inherit the threshold property. We can think of our construction as a compiler which takes as input two QSSSs (one fully quantum, one semi-quantum) realizing the same threshold access structure and outputs an MSSS. A natural question is to ask whether we can generalize our methodology to construct MSSSs to realize *general access structures*. Intuitively, it seems that given any general access structure (with the monotonicity property), if we use a QSSS realizing the given general access structure as a basic building block, then our proposed compiler construction can be extended to MSSS for general access structures. Constructions for QSSSs realizing general access structures exist in the literature [57, 58].

However, the existing schemes have certain limitations which make them difficult to be used in our case. For example, the scheme of [58] shares a classical secret in a quantum environment and hence cannot be used in our case to share the initial quantum secret. Also, our goal in this paper is to make our construction entanglement-free which we have been able to achieve in our construction. In [58], secret keys are encoded in the entangled GHZ states. While using quantum SSSs for general access structures, one should be careful to avoid the consequences of the "no-cloning theorem" so that no two disjoint groups of participants can reconstruct the secret hence violating the "no-cloning theorem" [17]. To summarize, instead of using a threshold QSSS as the underlying scheme, one may use a quantum scheme realizing a general access structure provided it can share a quantum secret in a quantum environment, satisfies the no-cloning theorem and does not use entanglement (or uses minimal amount of entanglement). The scheme of [57] discusses the concept of *quantum access structures* where along with monotonicity, any two qualified sets must have a non-empty intersection. There the authors also discuss decomposition of quantum access structures, improved maximal quantum access structures and present QSSSs realizing these access structures. So these QSSSs can be used in our construction but again these QSSSs use entanglement to a large extent and hence impose practical problems.

To the best of our knowledge, such a QSSS which completely fits the above-mentioned constraints of our construction and realizes any general access structure is still not available in the literature. We note that our compiler construction can be extended to realize general access structures when a general fully quantum secret sharing comes into existence. In this paper, we focus on threshold access structures and leave general access structures as a future work.

Another practical situation may arise. Since we can think of our construction as a compiler, let us suppose that a fully quantum threshold SSS is available to share the initial quantum secret and a semi-quantum SSS realizing a general access structure is available to share the natural number $\mathcal{X}$. A natural question can be put forward: can the constructed compiler work when two different QSSSs realizing two different access structures are presented ? We can definitely use the scheme of [58] which works for a general access structure. However, it may happen that a qualified set of participants (for threshold) reconstruct the initial state but this set is not qualified in other SSS that is being used to share the natural number. Hence, the natural number is not recovered, and as the result, the remaining secret quantum states are not reconstructed. This defeats the purpose of the of paper as the goal is to reconstruct the full set of secret quantum states. So a clarification regarding which subsets of participants are qualified when two different access structures are used simultaneously is required. This restricts the usage of QSSSs which realize arbitrary general access structures. This however does not rule out the possibility of using any other access structure instead of threshold access structures.

In [59], the authors have introduced the notions of improvable access structures and realizable restrictions of access structures which we think can be used in a situation where a mix of threshold access structure and a different access structure is required. We have only considered threshold QSSSs for our purpose and do not explore this possibility of this mix in this current work. We leave this interesting avenue for a future work.

5.2 Modifications for the multi-threshold variant

The above MSSS based on the discrete quantum walk model can be generalized to handle multi-threshold scenario as in the Procedures 1 and 2. Instead of sharing $\mathcal{X}$ by a one-shot threshold scheme, one may split the binary expansion of $\mathcal{X}$ into partitions and share the partitions among the participants in a similar manner as we have done in the case of procedure 1. This simple modification makes our scheme a multi-threshold SSS.

5.3 Application in the progressive setting

Let us suppose that the set of secrets be of the form $|\phi_{initial}\rangle = |\phi_1\rangle , |\phi_2\rangle , \ldots , |\phi_n\rangle = \left|\phi_{final}\right\rangle$. Let us also suppose that there is predefined notion of distance d. Examples of such distances can be found in [60]. In the progressive setting, it is required that for $(1 \leq i \leq n-1)$,

$$d(|\phi_i\rangle , |\phi_n\rangle) > d(|\phi_{i+1}\rangle , |\phi_n\rangle).$$

In this model, our constructions in procedures 1 and 2 can be directly applied to the effect that as more and more participants arrive, the reconstructed secret states get closer with respect to d to the final state $|\phi_n\rangle$. As we have noted in the sections following procedures 1 and 2 that existing relations between the states help in reducing

the dimensions of the share states, if there exists some known relations between the states (which is usually the case in visual secret sharing), the dimension of the share states can also be reduced in this case. In addition, we can make the scheme progressive by considering the methods in Sect. 4.7.

6 Security against adversarial attacks

Since we have assumed the existence of the underlying threshold quantum schemes(fully quantum and semi-quantum) [20, 21], our constructed scheme inherits the security provided by those schemes for example the intercept and resend attack, entangle and measure attack, man-in-the-middle attack, Trojan horse attack. The scheme of [21] is also a verifiable SSS, and hence, the participants can judge whether the recovered secret is the original one and check whether some dishonest participants provide the fake shadows in the reconstruction. Also, the use of trap code provides $(2/3)^{d/2}$ security against Pauli attacks [51, 52], where d is the distance of the underlying quantum error-correcting code used.

7 Comparison with existing schemes

The main difference of our scheme with the existing ones is that our scheme is a fully quantum MSSS. This means that the secrets are quantum states as opposed to semi-quantum schemes which share classical data. The achieved privacy, security and the dimension of the shares are unconditional, meaning that the results do not depend on the security of computationally hard problems like the lattice-based problems [13]. Our scheme works for discrete-time quantum walks for general graphs, as opposed to the construction in [33] which uses quantum walk over the circle graph and also the construction in [32] where the quantum walk is on a lattice folded into a torus. We also note that the schemes of [32] and [33] are not multi-SSSs and also are semi-quantum schemes. Also note that using the shunt decomposition model, one can construct multi-SSSs with potentially unbounded number of secrets.

In [59], the authors demonstrate a way to improve quantum SSSs by encrypting a quantum state $|S\rangle$ using a classical key K to obtain $\left|\tilde{S}\right\rangle$ and sharing $\left|\tilde{S}\right\rangle$ to only some selected participants and sharing the classical key K to some other participants via a classical SSS. For reconstruction, some participants recover K and the remaining participants using this key reconstruct $|S\rangle$ from $\left|\tilde{S}\right\rangle$. So one has to share less number of quantum states to the participants. This work was improved in [61] so that even more number of participants can carry classical shares. However, it was shown in [59] that this technique is not possible to be applied to various cases of quantum threshold schemes for example the 2-out-of-3 quantum threshold scheme. In this case, quantum states have to be shared to all three participants. The authors introduced the notion of an *improvable QSSS* which is a QSSS realizing an access structure Γ on a set of n participants and less than n quantum shares are sufficient to implement it. They proved that if a (n, k)-threshold scheme does not violate the no-cloning theorem, its

minimal access structure is equal to the optimal one and is given by the expression $(k-\gamma, n-\gamma)$ where $\gamma = 2k - n - 1$. By this formula, the *minimal restriction* [59] of a (99, 100) QTSS is a (2, 3) QTSS and only three quantum shares are required to implement a hybrid quantum secret sharing scheme realizing a quantum (99, 100)-threshold scheme.

We can similarly use this technique in our scheme to reduce the number of quantum shares given to the participants and decrease implementation costs. We can reduce the dimension of the shares given to each of the participants who only receive the classical shares. But for the participants who receive the quantum shares, the dimension does not reduce any further than our method. We have essentially reduced an MSSS to a single-SSS utilizing quantum walks. The role of the secret key K in [59] is very much different from the role of $\mathcal{X}$. We do not use $\mathcal{X}$ to recover the initial state $|\phi\rangle$ but rather to recover the remaining quantum secrets. The secret key K is comparable to the keys k_1 and k_2 corresponding to the permutation and the Pauli operator being used, respectively (See Definition 9). So for some of the participants receiving only these keys, the dimension of these participants can reduce to a some extent.

Also, this technique reduces the robustness of the construction. Since less number of quantum states are shared, the system is more susceptible to failure in case of errors arising from decoherence as compared to the case where all the participants have quantum shares.

8 Discussions

The main advantage of our construction is its generality. We are able to share multiple quantum secrets. Additionally, we have incorporated multi-threshold properties in the scheme, and our scheme is flexible enough to be used in a progressive model of secret sharing. All the schemes have been constructed keeping in mind the practical and implementation issues, and to this end, we have paid attention to the dimension of the share states in each of constructions. Table 1 compares the dimensions in each procedure and we see that assuming relations between the secret states is indeed advantageous. Our schemes inherit properties of the underlying threshold schemes [20, 21] both fully quantum and semi-quantum as they have been used without any modifications. This means that we get their security against adversarial attacks. Also, the scheme in [21] is a verifiable scheme, and hence, in our scheme also, we can verify if some participant presents wrong shares. The authors are unaware of any quantum scheme which assumes relation between secrets and suitably modifies the trap code. In the classical domain also while the technique of splitting the shares is quite prevalent [54], however, splitting the multiple secrets is not known to the authors.

9 Conclusion

We have given a compiler construction of an entanglement-free fully quantum multi-SSS which can accommodate a large number of participants into the system as opposed to entanglement-based methods. We have further showed that dimension of share states

Table 1 Comparison between dimensions

Procedure	Relation between quantum states	Dimension of share states
1 and 2	No relation	K^r, where $K = D_{\mathcal{S}} \times P_r \times \mu \times M$.
3 and 4	Single unitary operator	$D_{\mathcal{S}}^2$ ($\ll K^r$)
5 and 6	Quantum walk arc reversal	$D_{\mathcal{S}}^4$ or $D_{\mathcal{S}}^2$ (depending on model)
5 and 6	Quantum walk shunt decomposition	$D_{\mathcal{S}}^4$ or $D_{\mathcal{S}}^2$ (depending on model)

can be significantly reduced if we assume multiple secrets are related through quantum walk. In this paper, we have focussed on the threshold SSS and pointed out possible extensions to multi-threshold version of it. We leave open the interesting problems of extending the work to the case of multi-secret sharing in a mix of threshold and other access structures.

Acknowledgements The authors thank the anonymous reviewers whose careful and insightful comments helped in correcting various errors and largely improved the quality of the manuscript. The first author thanks TCG Centres for Research and Education in Science and Technology for a post-doctoral fellowship which financially supported this work. Second author was financially supported by MITACS Accelerate fellowship, Canada vide Ref. No. IT25625, FR66861. The authors also thank Bimal Kr. Roy and Goutam Mukherjee for stimulating discussions.

Data availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: International Workshop On Managing Requirements Knowledge, pp. 313–313. IEEE Computer Society (1979)
3. Blundo, C., Santis, A.D., Crescenzo, G.D., Gaggia, A.G., Vaccaro, U.: Multi-secret sharing schemes. In: Annual International Cryptology Conference, pp. 150–163. Springer (1994)
4. Dijk, M.V., Jackson, W.-A., Martin, K.M.: A general decomposition construction for incomplete secret sharing schemes. Des. Codes Cryptogr. **15**(3), 301–321 (1998)
5. Tartary, C., Pieprzyk, J., Wang, H.: Verifiable multi-secret sharing schemes for multiple threshold access structures. In: International Conference on Information Security and Cryptology, pp. 167–181. Springer (2007)
6. Dehkordi, M.H., Mashhadi, S.: New efficient and practical verifiable multi-secret sharing schemes. Inf. Sci. **178**(9), 2262–2274 (2008)
7. Beimel, A., Ben-Efraim, A., Padró, C., Tyomkin, I.: Multi-linear secret-sharing schemes. In: Theory of Cryptography Conference, pp. 394–418. Springer (2014)
8. Jackson, W.-A., Martin, K.M., O'Keefe, C.M.: Multisecret threshold schemes. In: Annual International Cryptology Conference, pp. 126–135. Springer (1993)
9. Masucci, B.: Sharing multiple secrets: models, schemes and analysis. Des. Codes Cryptogr. **39**(1), 89–111 (2006)
10. Waseda, A., Soshi, M.: Consideration for multi-threshold multi-secret sharing schemes. In: 2012 International Symposium on Information Theory and Its Applications, pp. 265–269. IEEE (2012)

11. Herranz, J., Ruiz, A., Sáez, G.: New results and applications for multi-secret sharing schemes. Des. Codes Cryptogr. **73**(3), 841–864 (2014)
12. Amroudi, A.N., Zaghain, A., Sajadieh, M.: A verifiable (k, n, m)-threshold multi-secret sharing scheme based on ntru cryptosystem. Wirel. Pers. Commun. **96**(1), 1393–1405 (2017)
13. Pilaram, H., Eghlidos, T.: A lattice-based changeable threshold multi-secret sharing scheme and its application to threshold cryptography. Sci. Iran. **24**(3), 1448–1457 (2017)
14. Hou, Y.-C., Quan, Z.-Y.: Progressive visual cryptography with unexpanded shares. IEEE Trans. Circuits Syst. Video Technol. **21**(11), 1760–1764 (2011)
15. Prasetyo, H., Hsia, C.-H., Wicaksono Hari Prayuda, A.: Progressive secret sharing with adaptive priority and perfect reconstruction. J. Imaging **7**(4), 70 (2021)
16. Anbarasi, L.J., Mala, G.A.: Survey and analysis of visual secret sharing techniques. Comput. Softw., p. 1507 (2014)
17. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**(4), 042311 (2000)
18. Mosca, M., Tapp, A., de Wolf, R.: Private quantum channels and the cost of randomizing quantum information (2000). arXiv:quant-ph/0003101
19. Lu, H., Zhang, Z., Chen, L.-K., Li, Z.-D., Liu, C., Li, L., Liu, N.-L., Ma, X., Chen, Y.-A., Pan, J.-W.: Secret sharing of a quantum state. Phys. Rev. Lett. **117**(3), 030501 (2016)
20. Qin, H., Zhu, X., Dai, Y.: (t, n) threshold quantum secret sharing using the phase shift operation. Quantum Inf. Process. **14**(8), 2997–3004 (2015)
21. Qin, H., Dai, Y.: Verifiable (t, n) threshold quantum secret sharing using d-dimensional bell state. Inf. Process. Lett. **116**(5), 351–355 (2016)
22. Song, X.-L., Liu, Y.-B., Deng, H.-Y., Xiao, Y.-G.: (t, n) threshold d-level quantum secret sharing. Sci. Rep. **7**(1), 1–9 (2017)
23. Qin, H., Tso, R., Dai, Y.: Multi-dimensional quantum state sharing based on quantum Fourier transform. Quantum Inf. Process. **17**(3), 1–12 (2018)
24. Mashhadi, S.: General secret sharing based on quantum Fourier transform. Quantum Inf. Process. **18**(4), 1–15 (2019)
25. Zhou, Q., Lv, H.: Multi-secret sharing model based on Hermite interpolation polynomial and quantum graph state. Int. J. Theor. Phys. **59**(8), 2271–2293 (2020)
26. Chen, H., Wu, H.-L., Chang, C.-C., Chen, L.-S.: Light repository blockchain system with multisecret sharing for industrial big data. Secur. Commun. Netw. **2019**(1), 7 (2019) https://doi.org/10.1155/2019/9060756
27. Mesnager, S., Sınak, A., Yayla, O.: Threshold-based post-quantum secure verifiable multi-secret sharing for distributed storage blockchain. Mathematics **8**(12), 2218 (2020)
28. Zhang, Z.-j, Li, Y., Man, Z.-x: Multiparty quantum secret sharing. Phys. Rev. A **71**(4), 044301 (2005)
29. Zhang, Z.-j, Man, Z.-x: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **72**(2), 022303 (2005)
30. Da-Zu, H., Zhi-Gang, C., Ying, G.: Multiparty quantum secret sharing using quantum Fourier transform. Commun. Theor. Phys. **51**(2), 221 (2009)
31. Smania, M., Elhassan, A.M., Tavakoli, A., Bourennane, M.: Experimental quantum multiparty communication protocols. Npj Quantum Inf. **2**(1), 1–4 (2016)
32. Karimipour, V., Asoudeh, M.: Quantum secret sharing and random hopping: using single states instead of entanglement. Phys. Rev. A **92**(3), 030301 (2015)
33. Lu, C., Miao, F., Hou, J., Ning, Y.: Quantum walk based quantum secret sharing in a verifiable framework. In: 2021 2nd International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE), pp. 271–276. IEEE (2021)
34. Guo, G.-P., Guo, G.-C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**(4), 247–251 (2003)
35. Yan, F.-L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A **72**(1), 012304 (2005)
36. Chandrashekar, C.M., Srikanth, R., Laflamme, R.: Optimizing the discrete time quantum walk using a su (2) coin. Phys. Rev. A **77**(3), 032326 (2008)
37. Childs, A.M.: On the relationship between continuous-and discrete-time quantum walk. Commun. Math. Phys. **294**(2), 581–603 (2010)
38. Szegedy, M.: Quantum speed-up of markov chain based algorithms. In: 45th Annual IEEE Symposium on Foundations of Computer Science, pp. 32–41. IEEE (2004)

39. Ambainis, A.: Quantum walk algorithm for element distinctness. SIAM J. Comput. **37**(1), 210–239 (2007)
40. Lovett, N.B., Cooper, S., Everitt, M., Trevers, M., Kendon, V.: Universal quantum computation using the discrete-time quantum walk. Phys. Rev. A **81**(4), 042330 (2010)
41. Godsil, C., Zhan, H.: Discrete-time quantum walks and graph structures. J. Comb. Theory Ser. A **167**, 181–212 (2019)
42. Watrous, J.: Quantum simulations of classical random walks and undirected graph connectivity. J. Comput. Syst. Sci. **62**(2), 376–391 (2001)
43. Aharonov, D., Ambainis, A., Kempe, J., Vazirani, U.: Quantum walks on graphs. In: Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, pp. 50–59 (2001)
44. Kendon, V.: Quantum walks on general graphs. Int. J. Quantum Inf. **4**(05), 791–805 (2006)
45. Yan, X., Lu, Y., Liu, L.: A general progressive secret image sharing construction method. Signal Process. Image Commun. **71**, 66–75 (2019)
46. Song, X., Wang, S., Sang, J., Yan, X., Niu, X.: Flexible quantum image secret sharing based on measurement and strip. In: 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 215–218. IEEE (2014)
47. Wang, H.-Q., Song, X.-H., Chen, L.-L., Xie, W.: A secret sharing scheme for quantum gray and color images based on encryption. Int. J. Theor. Phys. **58**(5), 1626–1650 (2019)
48. Portugal, R.: Quantum Walks and Search Algorithms, vol. 19. Springer, Berlin (2013)
49. Samadder Chaudhury, S.: A quantum evolving secret sharing scheme. Int. J. Theor. Phys. **59**(12), 3936–3950 (2020)
50. Chaudhury, S.S.: On quantum evolving secret sharing schemes-further studies and improvements. Quantum Inf. Comput. **21**(5&6), 0385–0407 (2022)
51. Broadbent, A., Gutoski, G., Stebila, D.: Quantum one-time programs. In: Annual Cryptology Conference, pp. 344–360. Springer (2013)
52. Broadbent, A., Wainewright, E.: Efficient simulation for quantum message authentication. In: International Conference on Information Theoretic Security, pp. 72–91. Springer (2016)
53. Broadbent, A., Jeffery, S.: Quantum homomorphic encryption for circuits of low t-gate complexity. In: Annual Cryptology Conference, pp. 609–629. Springer (2015)
54. Cheng, K., Ishai, Y., Li, X.: Near-optimal secret sharing and error correcting codes in ac0. In: Kalai, Y., Reyzin, L. (eds.) Theory of Cryptography—15th International Conference, TCC 2017, Baltimore, MD, USA, November 12–15, 2017, Proceedings, Part II (2017)
55. Komargodski, I., Naor, M., Yogev, E.: How to share a secret, infinitely. IEEE Trans. Inf. Theory **64**(6), 4179–4190 (2017)
56. Zhan, H.: Quantum walks on embeddings. J. Algebr. Comb. **53**(4), 1187–1213 (2021)
57. Bai, C.-M., Li, Z.-H., Si, M.-M., Li, Y.-M.: Quantum secret sharing for a general quantum access structure. Eur. Phys. J. D **71**(10), 1–8 (2017)
58. Wang, M.-M., Chen, X.-B., Yang, Y.-X.: Quantum secret sharing for general access structures based on multiparticle entanglements. Quantum Inf. Process. **13**(2), 429–443 (2014)
59. Nascimento, A.C., Mueller-Quade, J., Imai, H.: Improving quantum secret-sharing schemes. Phys. Rev. A **64**(4), 042311 (2001)
60. Dajka, J., Łuczka, J., Hänggi, P.: Distance between quantum states in the presence of initial qubit-environment correlations: a comparative study. Phys. Rev. A **84**(3), 032120 (2011)
61. Singh, S.K., Srikanth, R.: Generalized quantum secret sharing. Phys. Rev. A **71**(1), 012328 (2005)