New Protocols and Lower Bounds for Quantum Secret Sharing with Graph States

Jérôme Javelle[2], Mehdi Mhalla[1,2], and Simon Perdrix[1,2]

[1] CNRS
[2] LIG, Grenoble University, France

Abstract. We introduce a new family of quantum secret sharing protocols with limited quantum resources which extends the protocols proposed by Markham and Sanders [14] and Broadbent, Chouha, and Tapp [2]. Parametrized by a graph G and a subset of its vertices A, the protocol consists in: (i) encoding the quantum secret into the corresponding graph state by acting on the qubits in A; (ii) use a classical encoding to ensure the existence of a threshold. These new protocols realize $((k,n))$ quantum secret sharing i.e., any set of at least k players among n can reconstruct the quantum secret, whereas any set of less than k players has no information about the secret. In the particular case where the secret is encoded on all the qubits, we explore the values of k for which there exists a graph such that the corresponding protocol realizes a $((k,n))$ secret sharing. We show that for any threshold $k \geq n - n^{0.68}$ there exists a graph allowing a $((k,n))$ protocol. On the other hand, we prove that for any $k < \frac{79}{156}n$ there is no graph G allowing a $((k,n))$ protocol. As a consequence there exists n_0 such that the protocols introduced by Markham and Sanders in [14] admit no threshold k when the secret is encoded on all the qubits and $n > n_0$.

Keywords: Quantum Cryptography, Secret Sharing, Graphs, Graph States.

1 Introduction

Secret sharing schemes were independently introduced by Shamir [20] and Blakley [1] and extended to the quantum case by Hillery [10] and Gottesman [4,7]. A quantum secret sharing protocol consists in encoding a secret into a multipartite quantum state. Each of the players of the protocol has a *share* which consists of a subpart of the quantum system and/or classical bits. *Authorized* sets of players are those that can recover the secret collectively using classical and quantum communications. A set of players is *forbidden* if they have no information about the secret. The *accessing structure* is the description of the authorized and forbidden sets of players. The encrypted secret can be a classical bit-string or a quantum state.

A *threshold* $((k,n))$ quantum secret sharing protocol [10,4,7] is a protocol by which a dealer distributes shares of a quantum secret to n players such that any

K. Iwama, Y. Kawano, and M. Murao (Eds.): TQC 2012, LNCS 7582, pp. 1–12, 2013.

subset of at least k players is authorized, while any set of less than k players is forbidden. It is assumed that the dealer has only one copy of the quantum secret he wants to share. A direct consequence of the no-cloning theorem [22] is that no $((k,n))$ quantum secret sharing protocol can exists when $k \leq \frac{n}{2}$ – otherwise two distinct sets of players can reconstruct the secret implying a cloning of the quantum secret. On the other hand, for any $k > \frac{n}{2}$ a $((k,n))$ protocol has been introduced in [4] in such a way that the dimension of each share is proportional to the number of players. The unbounded size of the share is a strong limitation of the protocol, as a consequence several schemes of quantum secret sharing using a bounded amount of resources for each player have been introduced [14,2,13]. In [14] a quantum secret sharing scheme using particular quantum states, called *graph states*, and such that every player receives a single qubit, has been introduced. The graph-state-based protocols are also of interest because graph states are at the forefront in terms of implementation and have emerged as a powerful and elegant family of entangled states [9,21].

Only few threshold quantum secret sharing schemes have been proved in the literature to be achievable using graph states: $((3,5))$ can be done using a C_5 graph (cycle with 5 vertices) [14], and for any n, an $((n,n))$ protocol using the complete graph can be done, up to some constraints on the quantum secret [15]. Independently [2] introduced an $((n,n))$ protocol for any n. This protocol is based on the GHZ state [8] which is locally equivalent to a complete graph state [9].

We introduce a new family of secret sharing protocols using graph states. Like in [14] the quantum secret is encoded into a graph state shared between the players, but in order to obtain threshold protocols, an additional round is added to the protocol. This round consists in encrypting the quantum secret with a classical key which is then shared between the players using a classical secret sharing protocol. This technique extends the one presented in [2] in which the secret is partially encrypted and then shared using a fixed quantum state, namely the GHZ state which is equivalent to the complete graph state. The technique which consists in encrypting the quantum secret before to encode it into a larger state is also used in [16] in such a way that some players have a classical share but no quantum share.

The family of protocols we introduce in the present paper is parametrized by a pair (G,A) where $G=(V,E)$ is a graph and A is a non empty set of vertices of the graph. We explore the possible values of k for which there exists a pair (G,A) leading to a $((k,n))$ protocol. One of our main results is to introduce an infinite family of graphs which can realize any $((k,n))$ protocol when $k > n - n^{0.68}$. This result proves that graph states secret sharing can be used not only for $((n,n))$ protocols, but also for any threshold larger than $n - n^{0.68}$. The second main result of the paper is the proof that there is no graph G such that (G,V) realizes a $((k,n))$ protocols when $k < \frac{79}{156}n$. This lower bound also applies in the protocol introduced by Markham and Sanders. Moreover, it suggests that secret sharing protocols with a threshold closed to half of the players cannot be achieve with shares of bounded size.

In terms of communication complexity, the protocols we introduce use a maximal share of one qubit and two classical bits (using an ideal classical secret sharing scheme) for a one-qubit secret. In the literature, upper bounds for the information rate (size of the secret divided by the the size of the largest share) for general accessing structures have been derived in [18] and the analysis of different access structures have been studied in [19]. Independently, a hybrid classical-quantum construction of quantum secret sharing has been recently proposed in [6] where they optimize the quantum communication complexity when the size of the secret is greater than the number of players, and as a consequence, when the size of the shares is unbounded.

This paper is organized as follows. First, we present the schemes for sharing a classical (cQSS) or quantum (qQSS) secret using graph states as defined in [14]. We show that these cQSS protocols are perfect (every set of players is either authorized or forbidden), and we provide a graphical characterization of the accessing structures for both cQSS and qQSS protocols. Then, we extend these protocols and define a new family of perfect quantum secret sharing protocol (qQSS*). Finally, we prove upper and lower bounds for qQSS* threshold schemes: in section 3 we build a family of protocols that realize any $((k,n))$ threshold scheme for $k > n - n^{0.68}$; and in section 4, we prove that no qQSS* protocol can realize $((k,n))$ threshold scheme for $k < \frac{79}{156}n$. As a consequence, we derive an impossibility result for the existence of qQSS protocols.

2 Graph State Secret Sharing

2.1 Sharing a Classical Secret Using a Graph State

For a given graph $G = (V, E)$ with vertices $v_1, \ldots, v_n$, the corresponding graph state $|G\rangle$ is a n-qubit quantum state defined as

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q(x)} |x\rangle \tag{1}$$

where $q(x)$ is the number of edges in the induced subgraph $G^{(x)} = (\{v_i \in V \mid x_i = 1\}, \{(v_i, v_j) \in E \mid x_i = x_j = 1\})$.

Graph states have the following fundamental fixpoint property: given a graph G, for any vertex $u \in V$,

$$X_u Z_{N(u)} |G\rangle = |G\rangle \tag{2}$$

where $N(u)$ is the neighborhood of u in G, $X = |x\rangle \mapsto |\bar{x}\rangle$, $Z = |x\rangle \mapsto (-1)^x |x\rangle$ are one-qubit Pauli operators and $Z_A = \bigotimes_{u \in A} Z_u$ is a Pauli operator acting on the qubits in A. As a consequence, for any subset $D \subseteq V$ of vertices, $\bigotimes_{u \in D} X_u Z_{N(u)} |G\rangle = |G\rangle$. Since X and Z anti-commute and $Z^2 = X^2 = I$,

$$(-1)^{|D \cap Odd(D)|} X_D Z_{Odd(D)} |G\rangle = \bigotimes_{u \in D} X_u Z_{N(u)} |G\rangle = |G\rangle \tag{3}$$

where $Odd(D) := \{v \in V \ s.t. \ |N(v) \cap D| = 1 \bmod 2\}$ is the odd neighborhood of D. On occasion use of the graph G as subscript (N_G, Odd_G) will avoid ambiguity.

We study a family of quantum protocols for sharing a classical secret (cQSS) parametrized by a graph G and a non empty subset A of the vertices of the graph. This family of protocols has been introduced in [14]. Obviously, sharing a classical bit can be done using a classical scheme, like [20], instead of using a quantum state. It has been shown recently this family of cQSS protocols can be simulated by purely classical schemes [11]. However, the study of the cQSS protocols, and in particular the characterization of their accessing structure (see corollary 1) are essential for the next sections where the sharing of a quantum secret is considered.

To share a classical secret $s \in \{0,1\}$ between n players, the dealer prepares the state $|G_s\rangle = Z_A^s |G\rangle$ where $|G\rangle$ is a graph state on n qubits, Z_A^0 is the identity and Z_A^1 consists in applying the Pauli operator Z on each qubit of A. The dealer sends each player i the qubit q_i of $|G_s\rangle$. Regarding the reconstruction of the secret, a set B of players can recover the secret if and only if $tr(\rho_B(0)\rho_B(1)) = 0$, i.e. if the set of players can distinguish perfectly between the two states $\rho_B(0)$ and $\rho_B(1)$, where $\rho_B(s) = tr_{V\setminus B}(|G_s\rangle \langle G_s|)$ is the state of the subsystem of the players in B. On the other hand, a set B of players has no information about the secret if and only if $\rho(0)$ and $\rho(1)$ are indistinguishable, i.e. $\rho(0) = \rho(1)$.

Sufficient graphical conditions for a set to be authorized or forbidden have been proved in [12]:

Lemma 1 ([12]). *Given a cQSS protocol (G, A), for any $B \subseteq V$,*
– If $\exists D \subseteq B$ s.t. $D \cup Odd(D) \subseteq B$ and $|D \cap A| = 1 \bmod 2$ then B is authorized.
– If $\exists C \subseteq V \setminus B$ s.t. $Odd(C) \cap B = A \cap B$ then B is forbidden.

According to the previous lemma, for a given set of players $B \subseteq V$, if $\exists D \subseteq B$ s.t. $D \cup Odd(D) \subseteq B$ and $|D \cap A| = 1 \bmod 2$ then B can recover the secret. More precisely, the players in B perform a measurement of their qubits according to the observable $(-1)^{|D \cap Odd(D)|} X_D Z_{Odd(D)}$. This measurement produces a classical outcome $s \in \{0,1\}$ which is the reconstructed secret [12].

We prove that the sufficient graphical conditions are actually necessary conditions, and that the cQSS protocols are *perfect*, i.e. any set of players is either authorized or forbidden.

Theorem 1. *Given a graph $G = (V, E)$ and $A \subseteq V$, for any $B \subseteq V$, B satisfies exactly one of the two properties:*
i. $\exists D \subseteq B, D \cup Odd(D) \subseteq B$ *and* $|D \cap A| = 1 \bmod 2$
ii. $\exists C \subseteq V \setminus B, Odd(C) \cap B = A \cap B$

Proof. For a given $B \subseteq V$, let Γ_B be the cut matrix induced by B, i.e. the submatrix of the adjacency matrix Γ of G such that the columns of Γ_B correspond to the vertices in B and its rows to the vertices in $V \setminus B$. Γ_B is the matrix representation of the linear function which maps every $X \subseteq B$ to $\Gamma_B.X = Odd(X) \cap (V \setminus B)$, where the set X is identified with its characteristic column vector. Similarly, $\forall Y \subseteq V \setminus B$, $\Gamma_{V\setminus B}.Y = Odd(Y) \cap B$ where $\Gamma_{V\setminus B} = \Gamma_B^T$ since Γ

is symmetric. Moreover, notice that for any set $X, Y \subseteq V$, $|X \cap Y| \bmod 2$ is given by the matrix product $Y^T.X$ where again sets are identified with their column vector representation. Equation (i) is satisfied iff $\exists D$ s.t. $\left(\frac{(A\cap B)^T}{\Gamma_B}\right).D = \left(\frac{1}{0}\right)$ which is equivalent to $\mathsf{rank}\left(\frac{(A\cap B)^T}{\Gamma_B}\right) = \mathsf{rank}\left(\frac{(A\cap B)^T \mid 1}{\Gamma_B \mid 0}\right) = \mathsf{rank}\left(\frac{0 \mid 1}{\Gamma_B \mid 0}\right) = \mathsf{rank}(\Gamma_B) + 1$. Thus (i) is true iff $\pi(B) = 1$ where $\pi(B) := \mathsf{rank}\left(\frac{(A\cap B)^T}{\Gamma_B}\right) - \mathsf{rank}(\Gamma_B)$. Similarly equation (ii) is satisfied iff $\exists C$ s.t. $\Gamma_{V\setminus B}.C = A \cap B$ iff $\mathsf{rank}(\Gamma_{V\setminus B}|A \cap B) = \mathsf{rank}(\Gamma_{V\setminus B})$. Thus (ii) is true iff $\pi(B) = 0$. Since for any $B \subseteq V$, $\pi(B) \in \{0, 1\}$ it comes that either (i) is true or (ii) is true. □

Corollary 1. *Given a graph $G = (V, E)$, the cQSS protocol (G, A) is perfect and*

$$\begin{aligned} B \text{ is authorized} &\Leftrightarrow \exists D \subseteq B, D \cup Odd(D) \subseteq B \text{ and } |D \cap A| = 1 \bmod 2 \\ B \text{ is forbidden} &\Leftrightarrow \exists C \subseteq V \setminus B, Odd(C) \cap B = A \cap B \end{aligned}$$

2.2 Sharing a Quantum Secret

Following [14], the cQSS protocols are extended to qQSS schemes for sharing a quantum secret $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. Given a graph G and A a non empty subset of vertices, the dealer prepares the quantum state $|G_\phi\rangle = \alpha|G_0\rangle + \beta|G_1\rangle$. Notice that the transformation $|\phi\rangle \mapsto |G_\phi\rangle$ is a valid quantum evolution – i.e. an isometry – whenever $|G_0\rangle$ is orthogonal to $|G_1\rangle$ which is guaranteed by $A \neq \emptyset$. Then, the dealer sends each player i the qubit q_i of $|G_\phi\rangle$. Regarding the reconstruction of the secret, it has been proved in [14], that a set B of players can recover the quantum state $|\phi\rangle$ if and only if B can reconstruct a classical secret in the two cQSS protocols (G, A) and $(G\Delta A, A)$, where $G\Delta A = (V, E\Delta(A \times A))$ and $X\Delta Y = (X \cup Y) \setminus (X \cap Y)$ is the symmetric difference. In other words $G\Delta A$ is obtained by complementing the edges of G incident to two vertices in A. We introduce an alternative characterization of authorized sets of players (those who are able to reconstruct a quantum secret) which does not involved the complemented graph $G\Delta A$:

Theorem 2. *Given a graph $G = (V, E)$, a set B of players is authorized in the qQSS protocol (G, A) if and only if B is authorized and $V \setminus B$ is forbidden in the protocol cQSS (G, A).*

Proof. First notice that for any X, if $|X \cap A| = 1 \bmod 2$ then $Odd_{G\Delta A}(X) = Odd_G(X)\Delta A$. Thus for any X, Y, if $|X \cap A| = 1 \bmod 2$, $Odd_{G\Delta A}(X) \cap Y = \emptyset \iff (Odd_G(X)\Delta A) \cap Y = \emptyset \iff (Odd_G(X) \cap Y)\Delta(A \cap Y) = \emptyset \iff Odd_G(X) \cap Y = A \cap Y$.
($\Rightarrow$) Assume that B can reconstruct the quantum secret, so B can reconstruct the classical secret in $G\Delta A$. Thus $\exists D \subseteq B$ s.t. $Odd_{G\Delta A}(D) \cap (V \setminus B) = \emptyset$. According to the previous remark, it implies that $Odd_G(D) \cap V \setminus B = A \cap (V \setminus B)$, so $V \setminus B$ cannot reconstruct the secret.
($\Leftarrow$) Assume $V \setminus B$ cannot recover the classical secret and B can. So $\exists C \subseteq B$ s.t. $Odd_G(C) \cap B = A \cap B$. If $|C \cap A|$ is even, let $C' := C\Delta D$ where $|D \cap A|$

is odd and $Odd_G(D) \cap B = \emptyset$. Such a set D exists since B can reconstruct the classical secret in G. If $|C \cap A|$ is odd, then let $C' := C$. In both cases, $|C' \cap A| = 1 \bmod 2$ and $Odd_G(C') \cap B = A \cap B$, so according to the previous remark, $Odd_{G\Delta A}(C') \cap B = \emptyset$, as a consequence B is authorized secret in $G\Delta A$. □

In any pure quantum secret sharing protocol a set of players can reconstruct a quantum secret if and only if its complement set of players has no information about the secret (see [7]). As a consequence:

Corollary 2. *Given a qQSS protocol (G, A), a set B of players is forbidden if and only if B is forbidden and $V \setminus B$ is authorized in the protocol cQSS (G, A).*

Sets of players that can reconstruct the secret and those who have no information about the secret admit simple graphical characterisation thanks to the simple reduction to the classical case. However, unlike the cQSS case, there is a third kind of set players, those who can have some information about the secret but not enough to reconstruct the secret perfectly. For instance for any $n > 1$ consider the qQSS protocol $(K_n, \{v_1, \ldots, v_n\})$ where K_n is the complete graph on the n vertices $v_1, \ldots v_n$. For any set B of vertices s.t. $|B| \neq 0$ and $|B| \neq n$, both B and $V \setminus B$ cannot reconstruct a classical secret in the corresponding cQSS protocol, so B cannot reconstruct the quantum secret perfectly but has some information about the secret.

Corollary 3. *Given a graph $G = (V, E)$, the qQSS protocols (G, A) and $(G\Delta A, A)$ have the same accessing structure. In particular, the protocols (G, V) and $(\overline{G}, V)$ have the same accessing structure, where $\overline{G}$ is the complement graph of G.*

2.3 Threshold Schemes

Given a graph $G = (V, E)$ on n vertices and a non empty $A \subseteq V$, the accessing structures of the qQSS protocol (G, A) can be characterized. For secret sharing protocols, it is often interesting to focus on $((k, n))$ threshold protocols. In [7], it has been proved that if the dealer is sending a pure quantum state to the players, like in the qQSS protocols, then the threshold, if there exists, should be equal to $\frac{n+1}{2}$ where n is the number of players. This property which is derived from the no-cloning theorem, is very restrictive. It turns out that there is a unique threshold for which a qQSS protocol is known. This protocol is a ((3,5)) scheme using as graph the cycle graph on 5 vertices. However, in general a qQSS protocol corresponds to a ramp secret sharing scheme [17] where any set of players smaller than $n - k$ is forbidden and any set greater than k is authorized.

In this section we show how these ramp schemes can be turned into threshold schemes by adding a classical secret sharing round. First we define graphical properties that are used to characterize the access structures, then we prove that it is possible to build quantum threshold schemes by defining the protocols qQSS* that encodes the quantum secret in a subset of vertices A. Finally we

motivate the analysis of the case where the secret is encoded on all the vertices by giving a reduction from the general case where A is an arbitrary non empty subset of vertices.

Definition 1. *Given a graph $G = (V, E)$ of order n and $A \subseteq V$ a non empty subset of vertices. Let $\kappa_Q(G, A)$ be the minimal ℓ such that for any $B \subseteq V$, if $|B| > \ell$ then $\exists C_B, D_B \subseteq B$ such that: $|D_B \cap A| = 1 \bmod 2$, $Odd(D_B) \subseteq B$ and $Odd(C_B) \cap \overline{B} = A \cap \overline{B}$. We also define $\overline{\kappa_Q}(G, A) = n - \kappa_Q(G, A)$.*

Theorem 3. *Given a graph G over n vertices, a non empty subset of vertices A, and an integer $k > \kappa_Q(G, A)$, there exists an $((k + c, n + c))$ quantum secret sharing protocol for any $c \geq 0$ in which the dealer sends one qubit to n players and uses a $(k + c)$-threshold classical secret sharing scheme on the $n + c$ players.*

The rest of the section is dedicated to define a family of protocols called qQSS* satisfying the theorem.

Inspired by the work of Broadbent, Chouha and Tapp [2], we extend the qQSS scheme adding a classical reconstruction part. In [2], a family of unanimity – i.e. the threshold is the number of players – quantum secret sharing protocols have been introduced. They use a GHZ state which is equivalent to the graph state $|K_n\rangle$ where K_n is the complete graph on n vertices. We extend this construction to any graph, using also a more general initial encryption of the quantum secret.

Quantum Secret Sharing with Graph States and Classical Reconstruction (qQSS*). Given a graph $G = (V, E)$, a non empty $A \subseteq V$, and $k > \kappa_Q(G, A)$, suppose the dealer wishes to share the quantum secret $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$.

- **Encryption.** The dealer chooses uniformly at random $b_x, b_z \in \{0, 1\}$. and apply $X^{b_x} Z^{b_z}$ on $|\phi\rangle$.The resulting state is $|\phi'\rangle = \alpha |b_x\rangle + \beta(-1)^{b_z} |\overline{b_x}\rangle$.
- **Graph State Embedding.** The dealer embeds $|\phi'\rangle$ to the n-qubit state $\alpha |G_{b_x}\rangle + \beta(-1)^{b_z} |G_{\overline{b_x}}\rangle$.
- **Distribution.** The dealer sends each player i the qubit q_i. Moreover using a classical secret sharing scheme with a threshold k, the dealer shares the bits b_x, b_z.
- **Reconstruction.** The reconstruction of the secret for a set B of players s.t. $|B| \geq k$ is in 3 steps: first the set D_B such that $D \cup Odd(D) \subseteq B$ and $|D \cap A|$ is odd, is used to add an ancillary qubit and put the overall system in an appropriate state; then C_B such that $Odd(C) \cap (V \setminus B) = A \cap (V \setminus B)$, is used to disentangled the ancillary qubit form the rest of the system; finally the classical bits b_x and b_z are used to recover the secret:

  – (a) The players in B applies on their qubits the isometry $U_{D_B} := |0\rangle \otimes P_0 + |1\rangle \otimes P_1$ where P_i are the projectors associated with observable $\mathcal{O}_{D_B} = (-1)^{|D_B \cap Odd(D_B)|} X_{D_B} Z_{Odd(D_B)}$, i.e. $P_i := \frac{I + (-1)^i \mathcal{O}_{D_B}}{2}$. The resulting state is $\alpha |b_x\rangle \otimes |G_{b_x}\rangle + \beta.(-1)^{b_z} |\overline{b_x}\rangle \otimes |G_{\overline{b_x}}\rangle$.
  – (b) The players in B apply the controlled unitary map $\Lambda_{V_{C_B}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes V_{C_B}$, where $V_C := (-1)^{|C \cap Odd(C)|} X_C Z_{Odd(C) \Delta A}$. The resulting state is $\alpha |b_x\rangle \otimes |G\rangle + \beta.(-1)^{b_z} |\overline{b_x}\rangle \otimes |G\rangle = \left(\alpha |b_x\rangle + \beta.(-1)^{b_z} |\overline{b_x}\rangle\right) \otimes |G\rangle$.

– (c) Thanks to the classical secret sharing scheme, the players in B recover the bits b_x and b_z. They apply X^{b_x} and then Z^{b_z} for reconstructing the quantum secret $\alpha|0\rangle + \beta|1\rangle$ on the ancillary qubit.

Note that this reconstruction method can be used for the qQSS protocols defined in [12] and for which the reconstruction part was not explicitly defined.

Lemma 2. *Given a graph $G = (V, E)$, a non empty $A \subseteq V$, and $k > \kappa_Q(G, A)$, the corresponding qQSS* protocol is a $((k, n))$ secret sharing protocol, where $n = |V|$.*

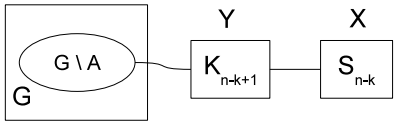
Proof. The classical encoding ensures that any set of size smaller then k is forbidden. $\mathcal{O}_{D_B}$ is acting on the qubits $D_B \cup Odd(D_B) \subseteq B$. Moreover $P_i|G_s\rangle = |G_s\rangle$ if $i = s$ and 0 otherwise, so the application of the isometry U_{D_B} produce the state $\alpha|b_x\rangle \otimes |G_{b_x}\rangle + \beta.(-1)^{b_z}\left|\overline{b_x}\right\rangle \otimes |G_{\overline{b_x}}\rangle$. Regarding step b of the reconstruction, since $Odd(C) \cap (V \setminus B) = A \cap (V \setminus B)$, $C \cup (Odd(C) \Delta A) \subseteq B$, so V_C is acting on the qubits in B. Moreover V_C produces the states $\left(\alpha|b_x\rangle + \beta.(-1)^{b_z}\left|\overline{b_x}\right\rangle\right) \otimes |G\rangle$. Finally the classical secret scheme guarantees that the players in B have access to b_x and b_z so that they reconstruct the secret. □

Proof of Theorem 3. The correctness of the qQSS* protocol implies that given a graph $G = (V, E)$ of order n, a non empty $A \subseteq V$, and $k > \kappa_Q(G, A)$, the corresponding qQSS* protocol is a $((k, n))$ secret sharing protocol. In order to finish the proof of Theorem 3 this protocol is turned into a $((k + c, n + c))$ protocol for any $c \geq 0$. The qQSS* protocol is modified as follows, following the technique used in [16]. During the distribution stage, the dealer shares b_x and b_z with all the $n + c$ players with a threshold $k + c$, but sends a qubit of the graph state to only n players chosen at random among the $n + c$ players. During the reconstruction, a set of $k + c$ players must contain at least k players having a qubit. These k players use the reconstruction steps (a) and (b) and then the last step (c) is done by all the $k + c$ players. □

In the next sections, we focus on the protocols of the form (G, V), where $G = (V, E)$. This restriction is motivated by the fact that, for any (G, A), there exists a graph $G' = (V', E')$ such that $\overline{\kappa_Q}(G', V') = \overline{\kappa_Q}(G, A)$. In other words:

Theorem 4. *If (G, A) realizes a $((k, n))$ qQSS* protocol, then there exists $G' = (V', E')$ such that (G', V') realizes a $((k + \ell, n + \ell))$ qQSS* protocol, where $\ell = 2n - 2k + 1$.*

Proof. Let $G' = (V', E')$ be the graph $G = (V, E)$ augmented with an independent set X of size $n - k$ and a clique Y of size $n - k + 1$, such that every vertex in Y is connected to the all the vertices in $X \cup (V \setminus A)$.



Let $B \subseteq V'$ s.t. $|B| = 2n - k + 1$. Since $|B \cap V| \geq k$, $\exists C, D \subseteq B \cap V$ s.t. $|D \cap A| = 1[2]$, $Odd(D) \cap V \subseteq B \cap V$, and $(Odd(C) \cap V' \setminus B) \cap V = (A \cap$

$V' \setminus B) \cap V$. We construct $C', D' \subseteq V'$ s.t. $|D'| = 1 \bmod 2$, $Odd(D') \subseteq B$ and $Odd(C') \cap V' \setminus B = V' \setminus B$ as follows:

– if $|D| = 1 \bmod 2$ then $|D \cap V' \setminus A| = 0[2]$ so $Odd(D) \cap Y = \emptyset$, thus $D' := D$.
– if $|D| = 0 \bmod 2$ and $B \cap X \neq \emptyset$, then $Y \subseteq Odd(D)$ and for any $x \in X \cap B$, $Odd(D \cup \{x\}) = Odd(D) \Delta N(x) \subseteq B$, so $D' := D \cup \{x\}$.
– if $|D| = 0 \bmod 2$ and $B \cap X = \emptyset$, then $B = V' \setminus X$, so for any $u \in V$, $Odd(\{u\}) \subseteq B$, thus $D' := \{u\}$.
– if $|C| = 0 \bmod 2$ then $Odd(C) \cap V' \setminus B = A \cap V' \setminus B$, thus for any $y \in Y \cap B$, $Odd(C \cup \{y\}) \cap V' \setminus B = V' \setminus B$, so $C' := C \cup \{y\}$.
– if $|C| = 1 \bmod 2$ and $X \cap B \neq \emptyset$ then for any $(x, y) \in (X \cap B) \times (Y \cap B)$, $Odd(C \cup \{x\} \cup \{y\}) \cap V' \setminus B = V' \setminus B$, so $C' := C \cup \{x\} \cup \{y\}$.
– if $|C| = 1 \bmod 2$, and $X \cap B = \emptyset$ then $V' \setminus B = X$, so for any $y \in Y$, $Odd(\{y\}) \cap V' \setminus B = V' \setminus B$, so $C' := \{y\}$. □

In the following, for any $G = (V, E)$, we consider protocols of the form (G, A) where $A = V$, as a consequence A is omitted in the notations e.g., $\kappa_Q(G)$ (resp. $\overline{\kappa_Q}(G)$) denotes $\kappa_Q(G, V)$ (resp. $\overline{\kappa_Q}(G, V)$).

3 Building $((n - n^{0.68}, n))$-qQSS* Protocols

We give a construction of an infinite family of quantum secret sharing schemes $((k, n))$ where $k = n - n^{\frac{log(3)}{log(5)}} < n - n^{0.68}$. To achieve this, we build a family of graphs G_i such that, for all i, $\overline{\kappa_Q}(G_i) \geq n^{0.68}$, where n is the order of G_i. This construction can be defined recursively from cycle over 5 vertices (C_5) which has been used in Markham and Sanders [14] to build a ((3,5)) quantum secret sharing protocol.

We recall the definition of the lexicographic product $\bullet$ between two graphs. Given $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, $G_1 \bullet G_2 = (V, E)$ is defined as $V := V_1 \times V_2$ and $E := \{((u_1, u_2), (v_1, v_2)) \mid (u_1, v_1) \in E_1 \text{ or } (u_1 = v_1 \wedge (u_2, v_2) \in E_2)\}$. In other terms, the graph G is a graph G_1 which vertices are replaced by copies of the graph G_2, and which edges are replaced by complete bipartitions between two copies of the graph G_2.

Lemma 3. *For any two graphs G_1, G_2, $\overline{\kappa_Q}(G_1 \bullet G_2) \geq \overline{\kappa_Q}(G_1).\overline{\kappa_Q}(G_2)$.*

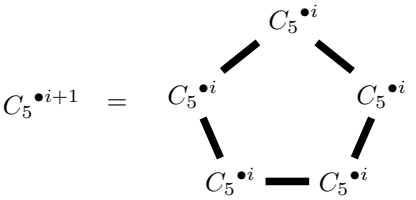
Proof. First we show that for any set $B \subseteq V$ of size k with $k = n_1 n_2 - \overline{\kappa_Q}(G_1)\overline{\kappa_Q}(G_2) + 1$ there exists a set D_B such that $|D_B| = 1 \bmod 2$, $Odd(D_B) \subseteq B$. For any set $B \subseteq V$ and any vertex $v_1 \in V$, let $B_2(v_1) = \{v_2 \in V_2 \ s.t. \ (v_1, v_2) \in B\}$ and $B_1 = \{v_1 \in V_1 \ s.t. \ |B_2(v_1)| > \kappa_Q(G_2)\}$. We claim that for all set $B \subseteq V$ of size $|B| = k$, the size of the set B_1 verifies $|B_1| > \kappa_Q(G_1)$. By contradiction, notice that $B = \bigcup_{v_2 \in B_2(v_1), v_1 \in V_1} \{(v_1, v_2)\}$. Therefore: $|B| = |V| - \sum_{v_1 \in B_1} |V_2 \setminus B_2(v_1)| - \sum_{v_1 \in V_1 \setminus B_1} |V_2 \setminus B_2(v_1)|$. Thus $|B| \leq n_1 n_2 - |V_1 \setminus B_1|.\overline{\kappa_Q}(G_2) \leq k - 1$ if $|B_1| < \kappa_Q(G_1)$. Now we consider any set $B \subseteq V$ of size $|B| = k$. As $|B_1| \geq k_1$, there exists a set $D_1 \subseteq B_1$ with $|D_1| = 1 \bmod 2$ and $D_1 \cup Odd(D_1) \subseteq B_1$. Furthermore for any $v_1 \in B_1$,

$|B_2(v_1)| > \kappa_Q(G_2)$ and thus there exists $D_2(v_1) \subseteq B_2(v_1))$ with $|D_2(v_1)| = 1 \bmod 2$ and $D_2(v_1) \cup Odd(D_2(v_1)) \subseteq B_2(v_1)$ and there exist $C_2(v_1) \subseteq B_2(v_1)$ with $V_2 \setminus B_2(v_1) \subseteq Odd(C_2(v_1)))$. Let $C_2^0(v_1) = C_2(v_1)$ if $|C_2(v_1)| = 0 \bmod 2$ and $C_2^0(v_1)\Delta D_2(v_1)$ otherwise, and let $C_2^1(v_1) = C_2^0(v_1)\Delta D_2(v_1)$. We partition V_1 in 4 subsets and define for any vertex v_1 a set $S_2(v_1) \subseteq V_2$ as follows

$$\begin{cases} \text{If } v_1 \in D_1 \cap (V_1 \setminus Odd(D_1)) & , S_2(v_1) = D_2(v_1) \\ \text{If } v_1 \in D_1 \cap Odd(D_1) & , S_2(v_1) = C_2^1(v_1)) \\ \text{If } v_1 \in V_1 \setminus (D_1 \cap (V_1 \setminus Odd(D_1))) & , S_2(v_1) = \varnothing \\ \text{If } v_1 \in V_1 \setminus (D_1 \cap Odd(D_1)) & , S_2(v_1) = C_2^0(v_1) \end{cases}$$

Consider the set $D_B = \bigcup_{v_1 \in V_1} \{v_1\} \times S_2(v_1)$, $D_B \subseteq B$ and $|D_B| = \sum_{v_1 \in D_1 \cap (V_1 \setminus D_1)} |D_2(v_1)| + \sum_{v_1 \in D_1 \cap Odd_(D_1)} |C_2^1(v_1)| + \sum_{v_1 \in V_1 \setminus D_1 \cap Odd(D_1)} |C_2^0(v_1)|$. Therefore $|D_B| = |D_1| = 1 \bmod 2$. For each $v = (v_1, v_2) \in V \setminus B$, $|\mathcal{N}_G(v) \cap D_B| = |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + \sum_{u_1 \in \mathcal{N}_{G_1}(v_1)} |S_2(u_1)|$. If $v_1 \in V_1 \setminus D_1$, then $|S_2(v_1)| = 0 \bmod 2$, thus $|\mathcal{N}_G(v) \cap D_B| = |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + |\mathcal{N}_{G_1}(v_1) \cap D_1| \mod 2$. Furthermore, if $v_1 \in V_1 \setminus D_1$, $|\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| = |\mathcal{N}_{G_1}(v_1) \cap D_1| = 0 \mod 2$ and if $v_1 \in Odd(D_1)$, $|\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| = |\mathcal{N}_{G_1}(v_1) \cap D_1| = 1 \mod 2$. Therefore $|\mathcal{N}_G(v) \cap D_B| = 0 \bmod 2$ which implies that $D_B \cup Odd(D_B) \subseteq B$. Furthermore, we use the property of the lexicographic product $\overline{G_1 \bullet G_2} = \overline{G_1} \bullet \overline{G_2}$. From Corollary 3 and Theorem 3, $\kappa_Q(G_1) = \kappa_Q(\overline{G_1})$ and $\kappa_Q(G_2) = \kappa_Q(\overline{G_2})$. Therefore, in $\overline{G_1 \bullet G_2}$ there exists a set D'_B such that its odd neighborhood in the complementary graph satisfies $Odd_{\overline{G_1 \bullet G_2}}(D'_B) \cap V \setminus B = \varnothing$ thus $Odd_{G_1 \bullet G_2}(D'_B) \cap V \setminus B = V \setminus B$ and D'_B is a valid C_B (as used in Definition 1) to define an $((k, n))$ qQSS* protocol. □

Theorem 5. *For all $i \in \mathbb{N}^*$, the graph $C_5^{\bullet i} = \underbrace{C_5 \bullet C_5 \bullet \cdots \bullet C_5}_{i \text{ times}}$ realizes a $((n, n - n^{\frac{log(3)}{log(5)}} + 1))$ protocol (with $n = 5^i$).*



Proof. An induction from Lemma 3 gives $\overline{\kappa_Q}(C_5^{\bullet i}) \geq \overline{\kappa_Q}(C_5)^i$. Since $\overline{\kappa_Q}(C_5) = 3$, $\overline{\kappa_Q}(C_5^{\bullet i}) \geq 3^i$. We have $|C_5^{\bullet i}| = 5^i$, so, thanks to Theorem 3, the graph $C_5^{\bullet i}$ realizes a $((n - n^{\frac{log(3)}{log(5)}} + 1, n))$ protocol (with $n = 5^i$). □

4 Lower Bound

By the no-cloning theorem, this is not possible to get two separated copies of the secret starting from only one copy. Thus, if we consider a quantum secret sharing protocol with parameters $((k, n))$ we must have $k > \frac{n}{2}$. We derive here less trivial lower bounds for the qQSS* protocols and for the qQSS protocols defined in [14].

Lemma 4. *If $G = (V, E)$ realizes a qQSS* $((k, n))$ protocol, then for any set $B \subseteq V$ of size k, there exists a set $X \subseteq B$ such that $|X| \leq \frac{2}{3}(n - k + 1)$ and either ($X \cup Odd(X) \subseteq B$ and $|X| = 1 \bmod 2$) or $B \subseteq Odd(X)$.*

Proof. First, let $\Gamma_B \in \mathcal{M}_{k,n-k}(\mathbb{F}_2)$ be a cut matrix of G corresponding to the cut $(B, V \setminus B)$. We can see Γ_B as the linear map that maps a set $D \subseteq B$ to its odd neighborhood in $V \setminus B$: Consequently, any set D with $D \cup Odd(D) \subseteq B$ corresponds to a linear combination of the columns of the matrix Γ_B which equals the null vector. Therefore, $\{D \subseteq B,\, D \cup Odd(D) \subseteq B\} = Ker(\Gamma_B)$, and $t = dim(Ker(\Gamma_B)) = k - dim(Im(\Gamma_B)) \geq 2k - n$. As $|X \Delta Y| = |X| + |Y| \bmod 2$, the sets $\mathcal{D}_1 = \{D \subseteq B, |D| = 1 \bmod 2 \text{ and } D \cup Odd(D) \subseteq B\}$ and $\mathcal{C}_1 = \{C \subseteq B, C \cup (V \setminus (C)) \subseteq B\}$ are two affine subspaces having the same vector subspace $\mathcal{D}_0 = \{D \subseteq B, |D| = 0 \bmod 2 \text{ and } D \cup Odd(D) \subseteq B\}$. The dimension of $\mathcal{D}_0$ is $t - 1$, therefore, by gaussian elimination its exists a set $X_0 \subseteq B$, $|X_0| = t - 1$ such that there exists sets $C_1 \in \mathcal{C}_1$ and $D_1 \in \mathcal{D}_1$ satisfying $X_0 \cap C_1 = X_0 \cap D_1 = \emptyset$. Thus $|C_1 \cup D_1| \leq k - t + 1 \leq n - k + 1$. Therefore $2|D_1 \cup C_1| = |D_1| + |C_1| + |D_1 \Delta C_1| \leq 2(n - k + 1)$ which implies that one of the three sets have cardinality smaller than $2(n - k + 1)$. as $D_1 \cup Odd(D_1) \subseteq B$ and $|D_1| = 1 \bmod 2$, $C_1 \cup (V \setminus Odd(C_1)) \subseteq B$ and $(D_1 \Delta C_1) \cup (V \setminus (D_1 \Delta C_1)) \subseteq B$ at least one of the has a cardinality smaller than $2(n - k + 1)/3$ □

Using this lemma and a counting argument we prove the following lower bound:

Theorem 6. *There exists no graph G that has a $((k, n))$ qQSS* protocol with $k < \frac{n}{2} + \frac{n}{157}$.*

Proof. We consider a graph $G = (V, E)$ which realizes a $((k, n))$ secret sharing protocol. Any set $D \subseteq V$, with $|D| = 1 \bmod 2$ satisfies $|D \cup Odd(D)| \geq n - k + 1$, otherwise $B = V \setminus (D \cup Odd(D)$ of size greater than k would not be authorized. Consequently, given a set D, with $|D| = 1 \bmod 2$, there exists at most $\binom{n-(n-k+1)}{k-(n-k+1)} = \binom{k-1}{2k-n-1}$ sets B of size k containing $D \cup Odd(D)$. Similarly, for any set $C \subseteq V$, $|C \cup (V \setminus Odd(C))| \geq n - k + 1$, otherwise $B = Odd(C) \setminus C$ of size greater than k would not be authorized. Therefore, given a set $C \subseteq V$ the number of sets B of size k containing C and such that $C \cup (V \setminus Odd(C)) \subseteq B$ is at most $\binom{k-1}{2k-n-1}$. With Lemma 4, each set $B \subseteq V$ of size k contains either a set D with $D \cup Odd(D) \subseteq B$ of size odd or a set C with $C \cup (V \setminus Odd(C)) \subseteq B$ such that $|D| \leq \frac{2}{3}(n - k + 1)$ or $|C| \leq \frac{2}{3}(n - k + 1)$. Thus by counting twice all the sets of cardinality smaller then $\frac{2}{3}(n - k + 1)$ we can upper bound the set of possible cuts of size k with $\binom{n}{k} \leq 2 \sum_{i=1}^{\frac{2}{3}(n-k+1)} \binom{n}{i} \binom{k-1}{2k-n-1}$. The previous inequality implies that $k > \frac{n}{2} + \frac{n}{157}$ when $n \to \infty$. □

The previous theorem directly implies that the protocols defined in [14] admit no threshold k when the secret is encoded on all the qubits and the number of players satisfies $n > 79$.

Corollary 4. *For any graph $G = (V, E)$ with $|V| \geq 79$, (G, V) is not a threshold qQSS protocol.*

Proof. By Gottesman's characterization [7] a qQSS protocol has a threshold $((k, 2k-1))$. Moreover, $k \geq n/2 + n/157$ using the previous lower bound. Therefore $k \leq 159/4$ and the number of players $n = 2k - 1 \geq 79$. □

References

1. Blakley, G.R.: Safeguarding cryptographic keys. In: AFIPS Conference Proceedings, vol. 48, pp. 313–317 (1979)
2. Broadbent, A., Chouha, P.R., Tapp, A.: The GHZ state in secret sharing and entanglement simulation. arXiv:0810.0259 (2008)
3. Browne, D.E., Kashefi, E., Mhalla, M., Perdrix, S.: Generalized flow and determinism in measurement-based quantum computation. New Journal of Physics 9, 250 (2007)
4. Cleve, R., Gottesman, D., Lo, H.-K.: How to Share a Quantum Secret. Phys. Rev. Lett. 83, 648–651 (1999)
5. Ekert, A.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67, 611 (1991)
6. Fortescue, B., Gour, G.: Reducing the quantum communication cost of quantum secret sharing. arXiv:1108.5541 (2011)
7. Gottesman, D.: On the Theory of Quantum Secret Sharing. Phys. Rev. A 61, 04231 (2000); also quant-ph/9910067
8. Greenberger, D.M., Horne, M.A., Zeilinger, A.: Going beyond Bells theorem. In: Bells Theorem, Quantum Theory, and Conceptions of the Universe, pp. 69–72 (1989)
9. Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states. Physical Review A 69, 062311 (2004); quant-ph/0307130
10. Hillery, M., Buzek, V., Berthiaume, A.: Quantum Secret Sharing Phys. Rev. A 59, 1829 (1999); arXiv/9806063
11. Javelle, J., Mhalla, M., Perdrix, S.: Classical versus Quantum Graph-based Secret Sharing arXiv:1109.4731 (2011)
12. Kashefi, E., Markham, D., Mhalla, M., Perdrix, S.: Information Flow in Secret Sharing Protocols. In: DCM 2009: Elec. Proc. Theor. Comp. Sci., vol. 9, p. 87 (2009)
13. Keet, A., Fortescue, B., Markham, D., Sanders, B.C.: Quantum secret sharing with qudit graph states. Phys. Rev. A 82, 062315 (2010)
14. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Physical Review A 78, 042309 (2008)
15. Markham, D., Sanders, B.C.: Erratum: Graph states for quantum secret sharing. Phys. Rev. A 78, 042309 (2008); Phys. Rev. A 83, 019901(E) (2011)
16. Nascimento, A., Mueller-Quade, J., Imai, H.: Improving quantum secret-sharing schemes. Phys. Rev. A 64, 042311 (2001)
17. Ogawa, T., Sasaki, A., Imamoto, M., Yamamoto, H.: Reducing the quantum communication cost of quantum secret sharing. Phy. Rev. A 72, 032318 (2005)
18. Sarvepalli, P.: Bounds on the information ate of quantum secret sharing. Phys. Rev. A 83, 042324 (2011)
19. Sarvepalli, P., Raussendorf, R.: Matroids and Quantum Secret Sharing Schemes Phys. Rev. A 81, 052333 (2010)
20. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
21. Raussendorf, R., Briegel, H.: A one-way quantum computer. Phys. Rev. Let. 86, 5188 (2001)
22. Wootters, W.K., Zurek, W.H.: A Single Quantum Cannot be Cloned. Nature 299, 802–803 (1982)