On the Capacity Region of Bipartite and Tripartite Entanglement Switching and Key Distribution

Gayane Vardoyan, Saikat Guha, Philippe Nain, Don Towsley

On the Capacity Region of Bipartite and Tripartite Entanglement Switching and Key Distribution

Gayane Vardoyan*, Saikat Guha†, Philippe Nain‡, and Don Towsley*
* College of Information and Computer Sciences, University of Massachusetts, Amherst, {gvardoyan, towsley}@cs.umass.edu
†College of Optical Sciences, The University of Arizona, saikat@optics.arizona.edu
‡ Inria, France, philippe.nain@inria.fr

We study a quantum switch serving a set of users. The function of the switch is to convert bipartite entanglement generated over individual links connecting each user to the switch, into bipartite or tripartite entangled states among (pairs or groups of) users at the highest possible rates at a fixed ratio. Such entanglement can then be converted to quantum-secure shared secret bits among pairs or triples of users using E91-like Quantum Key Distribution (QKD) protocols. The switch can store a certain number of qubits in a quantum memory for a certain length of time, and can make two-qubit Bell-basis measurements or three-qubit GHZ-basis projective measurements on qubits held in the memory. We model a set of randomized switching policies. Discovering that some are better than others, we present analytical results for the case where the switch stores one qubit per user at a given time step, and find that the best policies outperform a time division multiplexing (TDM) policy for sharing the switch between bipartite and tripartite entanglement generation. This performance improvement decreases as the number of users grows. The model is easily augmented to study the capacity region in the presence of qubit decoherence, obtaining similar results. Moreover, decoherence appears to have little effect on capacity. We also study a smaller class of policies when the switch can store two qubits per user. The full manuscript can be found at https://arxiv.org/abs/1901.06786.

Multi-qubit entangled states are fundamental building blocks for quantum computation, sensing, and security. Consequently there is a need for a quantum network that can generate such entanglement on demand between pairs and groups of users [1]–[3]. In this work, we study the performance of the simplest multi-user network, a star-topology quantum switch connecting k users, where each user is connected to the switch via a separate optical link as shown in Figure 1. Bipartite, two-qubit maximally-entangled states, *i.e.*, Bell pairs (or EPR states) are generated at a constant rate across each link, with the qubits getting stored at local quantum memories at each end of the links. As these link entanglements start appearing, the switch uses two-qubit Bell-state measurement (BSM) between pairs of locally-held qubits and three-qubit Greenberger-Horne-Zeilinger (GHZ) basis measurements between triples of locally-held qubits to provide two-qubit and three-qubit entanglements to pairs and triples of users, respectively [4]. The capacity of such a switch to provide these two types of entanglements to the users depends on the switching mechanism, the number of quantum memories and their decoherence rates, and the number of links.

Using the Ekert-91 (E91) protocol for Quantum Key Distribution (QKD) [5], pairs of users can convert shared Bell states into shared secret bits whose security derives from quantum mechanics. Similarly, a variant of the E91 protocol can be employed to convert shared GHZ states between three users into tripartite quantum-secured shared secret bits. If QKD is the ultimate goal of the quantum network, the end users do not need to have quantum memories. They can keep making projective measurements chosen randomly from a set of mutually-unbiased measurement bases as specified in the E91 protocol, and extract shared keys in post-processing using reconciliation, error correction and privacy amplification. Since shared key generation is a strictly weaker task than entanglement generation, an entanglement distribution rate is always also an achievable rate for QKD. Therefore, hereon in this paper, we will focus exclusively on entanglement generation rates.

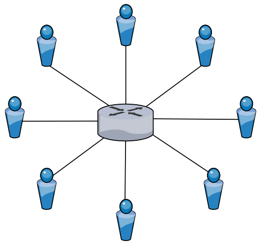


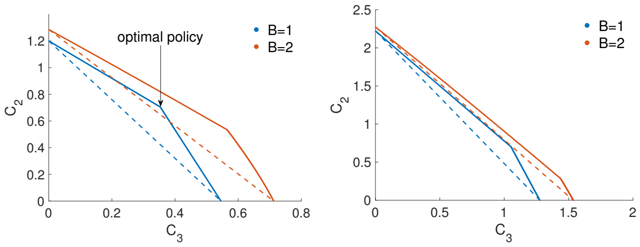
Fig. 1: A quantum switch serving k users in a star topology.

The creation of an end-to-end entanglement requires two steps. First two-qubit Bell states are generated pairwise between a qubit stored locally at the switch and a qubit owned by a user. Once such link-level two-qubit entangled states have been created, the switch performs joint (entangling) measurements (over $j \geq 2$ locally-held qubits that are entangled with qubits held by j distinct users), which, if successful, produces a j-qubit maximally-entangled state between the corresponding j users. After the measurement, if the result of the measurement is communicated to the end nodes, they can use conditional local unitaries on their qubits to convert the shared entanglement into a generic pre-determined j-qubit GHZ state of their choice. Link-level entanglement generation, as well as entangling measurements, when realized with practical systems, are inherently probabilistic [6]. We assume that only two-user (two-qubit) and three-user (three-qubit) entanglements are created, i.e., 2-qubit BSMs and 3-qubit GHZ basis measurements are done at the switch. For simplicity, we assume that these $j = 2$ or 3 qubit measurements at the switch take negligible time and always succeed.

Each link attempts two-qubit entanglements in each time slot of length τ seconds, and with probability p, establishes one entangled pair successfully. For simplicity, we model the time to successfully create a link entanglement as an exponential random variable with mean $1/\mu = \tau/p$. We assume that each link can store $B = 1, 2, \ldots$ qubits. We also assume that qubits at the switch can decohere and model decoherence time as an exponential random variable with mean $1/\alpha$. We assume a step-function decoherence model where the two-qubit entanglement goes from a maximally-entangled qubit pair (one ebit) to zero entanglement. In this work, we only consider $B = 1, 2$. Last, when a qubit is stored at the switch, with its entangled pair stored at a user, we refer to this as a *stored link entanglement*.

We assume that all possible bipartite and tripartite user entanglements are of interest and consider two classes of probabilistic policies, one for $B = 1$ and the second for $B = 2$, that provide the flexibility to generate both types of entanglements with arbitrary rates. Policies in both classes incorporate the *oldest link entanglement first* (OLEF) rule whereby when a link entanglement is created it is always matched up with stored link entanglements when possible rather than be stored. This has the nice consequence, when coupled with the assumption that links are homogeneous but statistically independent, that the system can be modeled by a continuous time Markov chain (CTMC) where the state simply tracks the number of stored entanglements for two users. Moreover, the OLEF rule ensures an efficient use of resources (*i.e.*, link-level entanglements) in the presence of decoherence.

In this work, we employ a set of time division multiplexing (TDM) policies as a baseline. When operating according to a TDM policy, the switch performs BSMs γ fraction of the time and tripartite GHZ basis measurements $1-\gamma$ fraction of the time, for $\gamma \in [0, 1]$. The goal is to determine whether there exist policies that yield higher switch capacity than TDM policies. To this end, we consider a class of randomized policies. When properly configured, these randomized policies outperform TDM. However the relative difference between the two randomized policies and TDM goes to zero as the number of links $k \to \infty$. We also observe that increasing the number of memories from one to two increases capacity but that the advantage diminishes as k gets large. We also explore the effect that decoherence—the locally stored qubits at each end of the link being subject to a noise process that reduces the entanglement between the two qubits—has on capacity.



(a) $k = 3$

(b) $k = 5$

Fig. 2: Comparison of capacity regions for systems of buffer sizes one and two with varying number of links k, and entanglement generation rate $\mu = 1$.

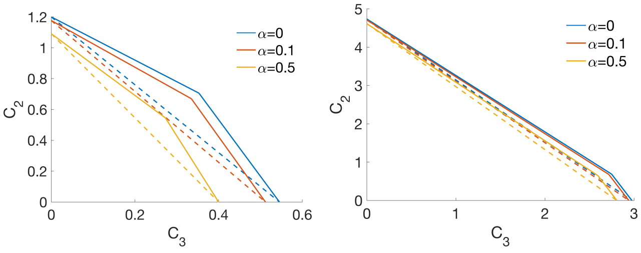
In the cases of $B = 1$ with and without decoherence, we have simple closed form expressions for capacity whereas for the case of $B = 2$, our results are numerical. Both types of systems are modeled using CTMCs and capacities of bipartite and tripartite end-to-end entanglements are computed using the stationary distributions. An example of the capacity regions for $B = 1, 2$ is shown in Figure 2. In the figure, C_2 represents the bipartite capacity and C_3 the tripartite capacity. Note that the entanglement generation rate simply scales the capacities by μ, so we have set it equal to 1 for all examples shown. For the case of $B = 1$, we study the entire capacity region of the switch under a set of randomized policies that enable the switch to make more diverse decisions than the set of TDM policies. While we find many such policies that outperform TDM, one in particular stands out: a policy that yields the most efficient operation in terms of optimizing both bipartite and tripartite entanglement capacities. This policy is labeled in Figure 2a and can be stated as follows:

(i) Suppose there is currently only one stored link entanglement. Let l_1 be the link that is associated with this entanglement. When another link (not l_1) generates an entanglement, the switch should store it (as opposed to using the two link-level entanglements in a BSM). Note that if l_1 is the link that generates a new entanglement, the older (stored) one is dropped by the switch since $B = 1$, and the newer one is stored for future use.

(ii) Suppose that there are currently two stored link-level entanglements (note that since $B = 1$, they must belong to two different links). Let l_1 and l_2 be the two links associated with these entanglements. If another link, l_3 generates an entanglement, the switch must always use the three distinct link-level entanglements to serve a tripartite end-to-end entanglement between the three users. However, if either l_1 or l_2 generates another entanglement, the switch must *always* perform a BSM using the two stored entanglements, and the new entanglement is stored for future use. Note that the latter rule directs the switch to not waste an entanglement whenever it is possible to use it in a measurement.

For $B = 1$, we analytically show that this policy is optimal. Further, we derive tight upper bounds on the achievable capacities given the set of randomized policies considered in this work. Note that the set of TDM policies form a line connecting the maximum achievable bipartite capacity, C_2^*, and the maximum achievable tripartite capacity, C_3^*. C_2^* and C_3^* are obtained when the switch performs only BSMs or 3-qubit GHZ basis measurements, respectively. We call this the TDM line. Let the point $(\hat{C}_3, \hat{C}_2)$ represent the tripartite and bipartite capacity produced by the optimal policy described above. We show that the upper bounds on the achievable capacity form a triangular region above the TDM line, such that the vertex of the triangle is the point $(\hat{C}_3, \hat{C}_2)$, *i.e.*, the point farthest away from the TDM line. Denote the area of the triangular capacity region above the TDM line as $A_\triangle$, and the area below the TDM line as A_{TDM}. Then the total area of the achievable capacity region is $A_T = A_\triangle + A_{TDM}$. We show that as $k \to \infty$, $A_\triangle / A_T \to 0$. This result is proof that as the number of links grows, the advantages of using the alternate, randomized policies as opposed to TDM diminish.

For the case $B = 1$, the set of policies that we explored was exhaustive; *i.e.*, we consider every policy that can be modeled by the CTMC. For the case $B = 2$, we opt for a less exhaustive search, but the goal is the same: determine whether there exist policies that perform better than TDM. Our analysis of this system is numerical, but the results closely resemble those of the $B = 1$ case: there is a region above the TDM line that represents a set of policies which outperform TDM. Also, as k increases, we observe that the ratio of the region above the TDM line to the achievable capacity region decreases. Moreover, we compare the capacity regions obtained from the $B = 1$ and $B = 2$ systems and discover while there is something to be gained from the extra buffer space for a small number of users, the advantage becomes less apparent for a larger number of users.

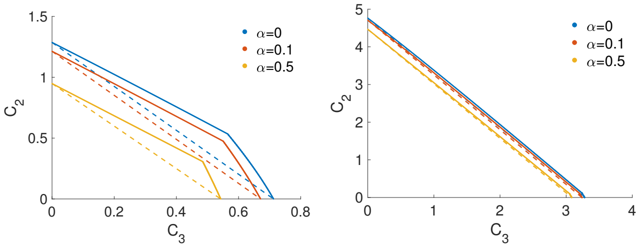


(a) $k = 3$

(b) $k = 10$

Fig. 3: Capacity region for a system of buffer size one and varying number of links k, decoherence rates α, and entanglement generation rate $\mu = 1$. The solid lines are the upper boundaries of the capacity region, and the dashed are TDM lines.

Another contribution of this work is a simple way to model the phenomenon of the decoherence of quantum states. For the two existing systems with $B = 1$ and $B = 2$, we introduce a new parameter, α, which represents the rate of decoherence.



(a) $k = 3$

(b) $k = 10$

Fig. 4: Capacity region for a system of buffer size two and varying number of links k, decoherence rates α, and entanglement generation rate $\mu = 1$. The solid lines are the upper boundaries of the capacity region, and the dashed are TDM lines.

For $B = 1$, the analysis of the capacity region is very similar to the original system without decoherence. As one expects, the effect of decoherence is that the achievable capacity region shrinks as α increases. Interestingly, we observe that this effect also diminishes as the number of links k grows. Examples of this phenomenon are shown for $B = 1$ and $B = 2$ in Figures 3 and 4, respectively. For all examples, we use an entanglement generation rate of $\mu = 1$; for qualitative results, we only need to concern ourselves with the value of α *relative* to μ. In typical scenarios, α is at least one order of magnitude smaller than μ.

To summarize, in this work, we explore a set of policies for a quantum switch that can store up to two qubits per link and whose objective is to perform bipartite and tripartite joint measurements to distribute two and three qubit entanglement to pairs and triples of users. We present analytical results for the case where the per-link buffer has size one. By comparing against TDM policies, we discover that better policies in terms of achievable bipartite and tripartite capacities exist, but that as the number of links grows, the advantage of using such policies diminishes. We also compare the capacity regions for systems with different per-link buffer sizes and observe that systems with fewer links benefit more from the extra storage space than systems with a larger number of links. Finally, we model decoherence for both types of systems and present analytical results for the case with per-link buffer size one. Observations and analysis show that as the number of links increases, the effects of decoherence become less apparent on systems.

References

[1] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Routing Entanglement in the Quantum Internet," 2019.

[2] E. Schoute, L. Mancinska, T. Islam, I. Kerenidis, and S. Wehner, "Shortcuts to quantum network routing," Oct. 2016.

[3] R. Van Meter, *Quantum networking*. John Wiley & Sons, 2014.

[4] M. A. Nielsen and I. Chuang, "Quantum Computation and Quantum Information," 2002.

[5] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.

[6] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater *et al.*, "Rate-loss Analysis of an Efficient Quantum Repeater Architecture," *Phys. Rev. A.*