Entanglement Generation in a Quantum Network at Distance-independent Rates

Center for Quantum Networks

Ashlesha Patil[1], Mihir Pant[2], Dirk Englund[2], Don Towsley[3] and Saikat Guha[1]

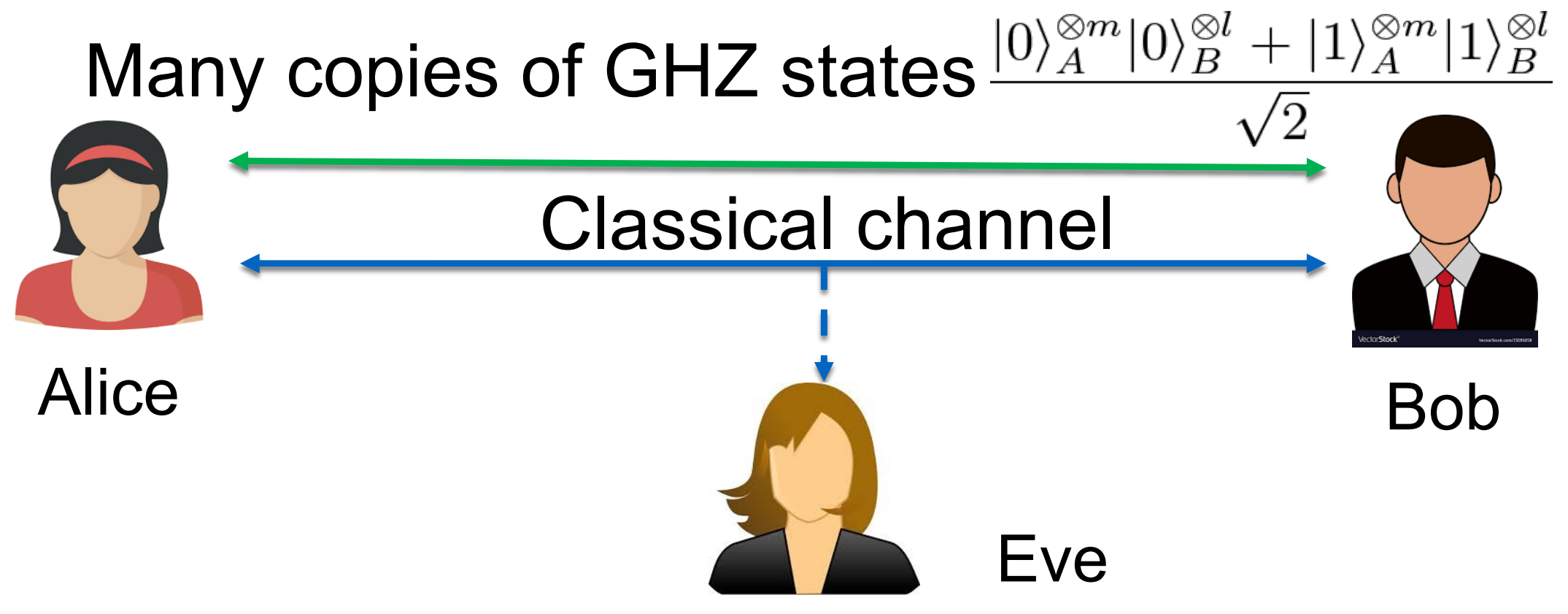
[1]James C. Wyant College of Optical Sciences, University of Arizona, 1630 E University Blvd., Tucson, Arizona 85721, USA.
[2]*Massachusetts Institute of Technology, 32 Vassar Street, Cambridge MA 02139, USA.*
[3]*College of Information and Computer Sciences, University of Massachusetts, Amherst, MA 01002, USA.*

arXiv:2005.07247

In a nutshell

- We develop a new QKD protocol that allows a pair of users to sift a secret key starting from shared variable length Greenberger-Horne-Zeilinger (GHZ) states.
- An entanglement generation scheme that achieves **rates that are independent of the distance** between the two users, despite lossy (hence probabilistic) link-level entanglement generation, and probabilistic success of the projective measurements at repeaters.
- The key new insight in our protocol is **to allow a repeater node to use *n*-qubit GHZ projective measurements** that can fuse n successful entangled *links*.
- The distance-independent rate is not possible to attain with any quantum networking protocol using Bell measurements and multiplexing alone.

The QKD Protocol



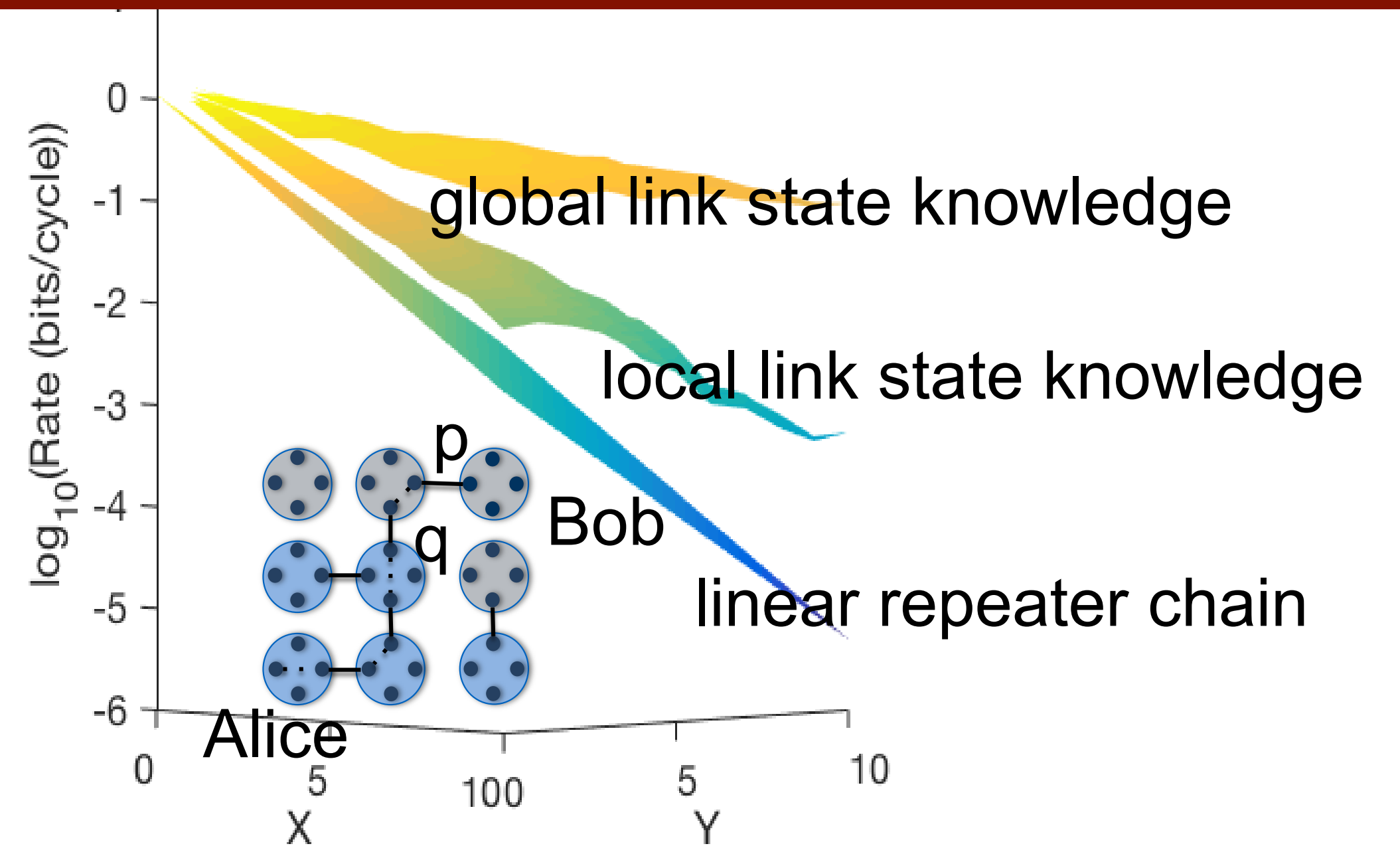
	Alice			Bob	
Basis	Measurement outcome	Key	Basis	Measurement outcome	Key
+/-	1010	0	+/-	0	0
0/1	0	0	0/1	0	0
+/-	1101	-	0/1	11	-
+/-	100	1	+/-	010	1
0/1	1111	-	+/-	01	-
0/1	111	1	0/1	111	1
0/1	00	-	+/-	110	-

- Extension of the BBM'92 protocol [1].
- ***Step 1:*** Alice and Bob start with multiple $m + l \geq 2$ qubit GHZ states such that Alice and Bob have m- and l qubits of the GHZ state. Here, m and l can vary across the collection of shared GHZ states Alice and Bob possess.
- ***Step 2:*** Each user measures all their qubits of the GHZ state using (their) independently and randomly-chosen measurement basis.
- ***Step 3:*** If both of them used

a. the (0/1-basis), they get bit string of either all 0's or all 1's. In this case, that bit becomes the key.

b. the (+/- - basis), the key is the parity of their respective measurement outcome bit strings.

Entanglement Routing using Bell-State Measurements

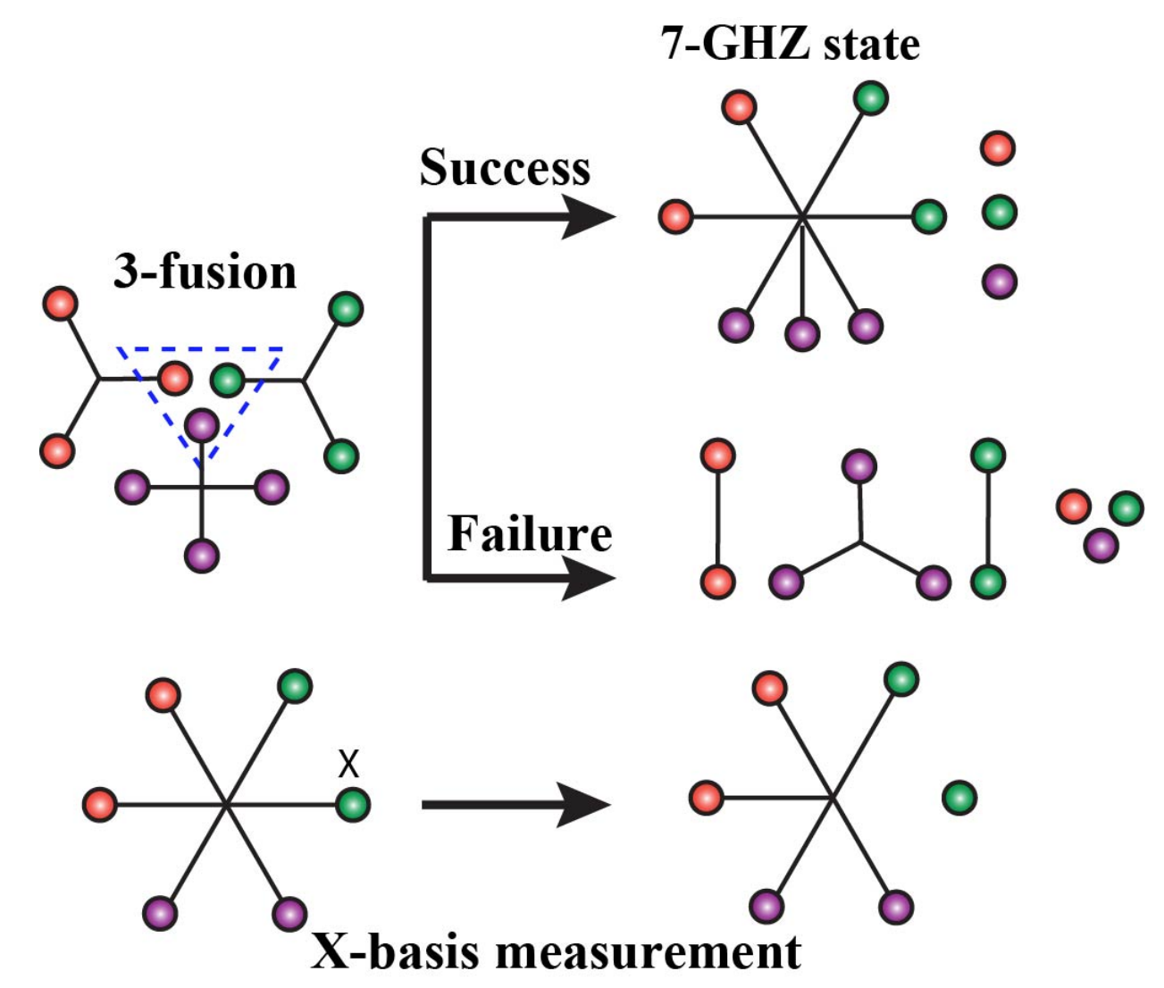


p – link generation probability
q – Bell state measurement success probability

- Higher rate compared to linear repeater chain along shortest path, even using local link state knowledge [2]
- Entanglement rate decays exponentially even with global link state knowledge when q <1 [2].

Distance-Independent Entanglement Generation Rate

Measurements used -



Note that these are not cluster states.

(i) ***k*-fusion** – joint projective measurement on the GHZ basis performed on *k*-qubits from Bell/GHZ states. If

successful – creates a GHZ state among all the unmeasured qubits

fails – due to hardware constraints, we model it by performing X-basis measurements on the *k*-qubits.

(ii) **X-basis measurement** removes the qubit from the GHZ state

The *n*-GHZ protocol -

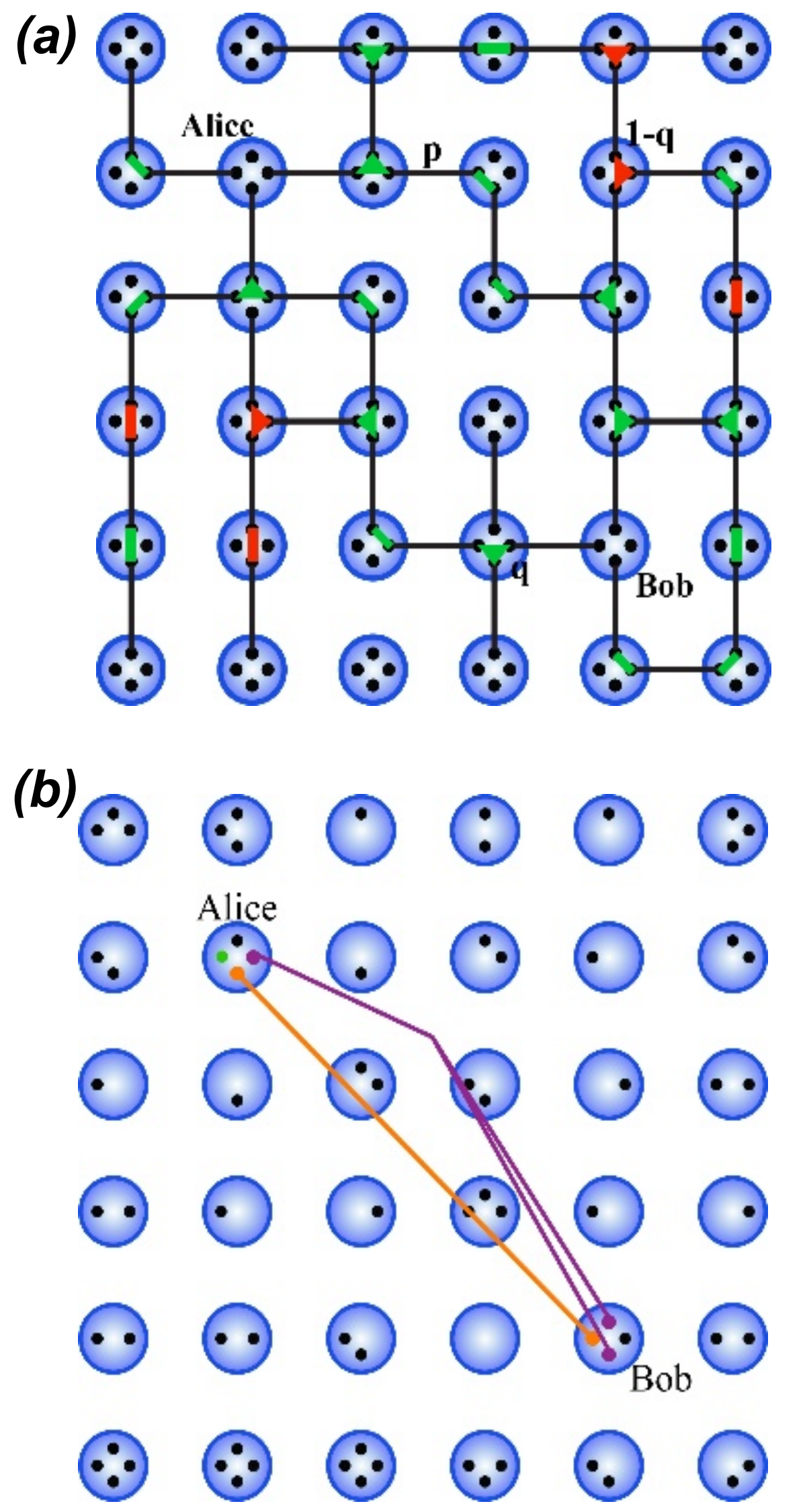


Fig. 1 – 3-GHZ protocol on square-grid network

(i) *Link (*shared Bell pair between neighboring repeaters) generation attempts at each repeater, i.i.d., with success probability *p*.

(ii) The repeater nodes have only *local link-state knowledge.*

(iii) *k*-fusion attempts at each repeater except Alice and Bob, i.i.d., with success probability *q*

- *k = min(n, no. of successful links at the repeater)*
- if *k = 1,* X-basis measurement
- The fusions and the X-basis measurements occur simultaneously.

Implementing *k*-fusion, for *k*≥3 is in principle not much harder than 2-fusions (Bell measurement) in qubit memories, e.g., color centers in diamond [3].

(iv) GHZ states shared between Alice and Bob

Shared entanglement is generated if there exists at least one path between Alice and Bob in the (network) graph of qubits generated after fusions. (*Fig. 1(a)*) – Site-bond **Percolation!**

- Site occupation probability ≡ *q*, bond occupation probability ≡ *p*

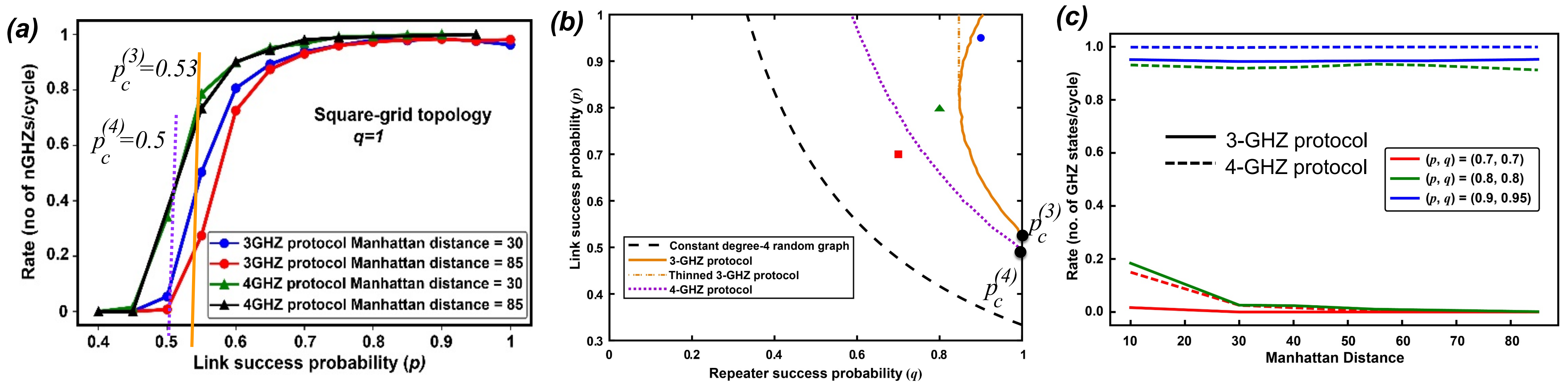


Fig. 2 – (a) shows that after p crosses a threshold p_c , as dictated by the site-bond region, the rate goes from near zero (regime where rate falls exponentially) to 1. (b) (p,q) region where our protocol supports distance-independent entanglement rate (c) Rate as a function of distance for three different values of (p.q) marked in (b).

When *(p, q)* lies in the super-critical regime of the relevant percolation problem, the end-to-end entanglement rate becomes independent of the distance between Alice and Bob.

References: [1] Bennet, C. H., Brassard, G., and Mermin, N., D., Phys. Rev. Lett. 68, 1992, pp. 557-559.
[2] Pant, M., Krovi, H., Towsley, D., Tassiulas, L., Jiang, L., Basu, P., Englund, D. and Guha, S., *npj Quantum Information*, *5*(1), 2019
[3] M. Bhaskar, *et al.*, Nature 580 (7801), 60-64(2020).