Modeling and performance evaluation of a quantum switch

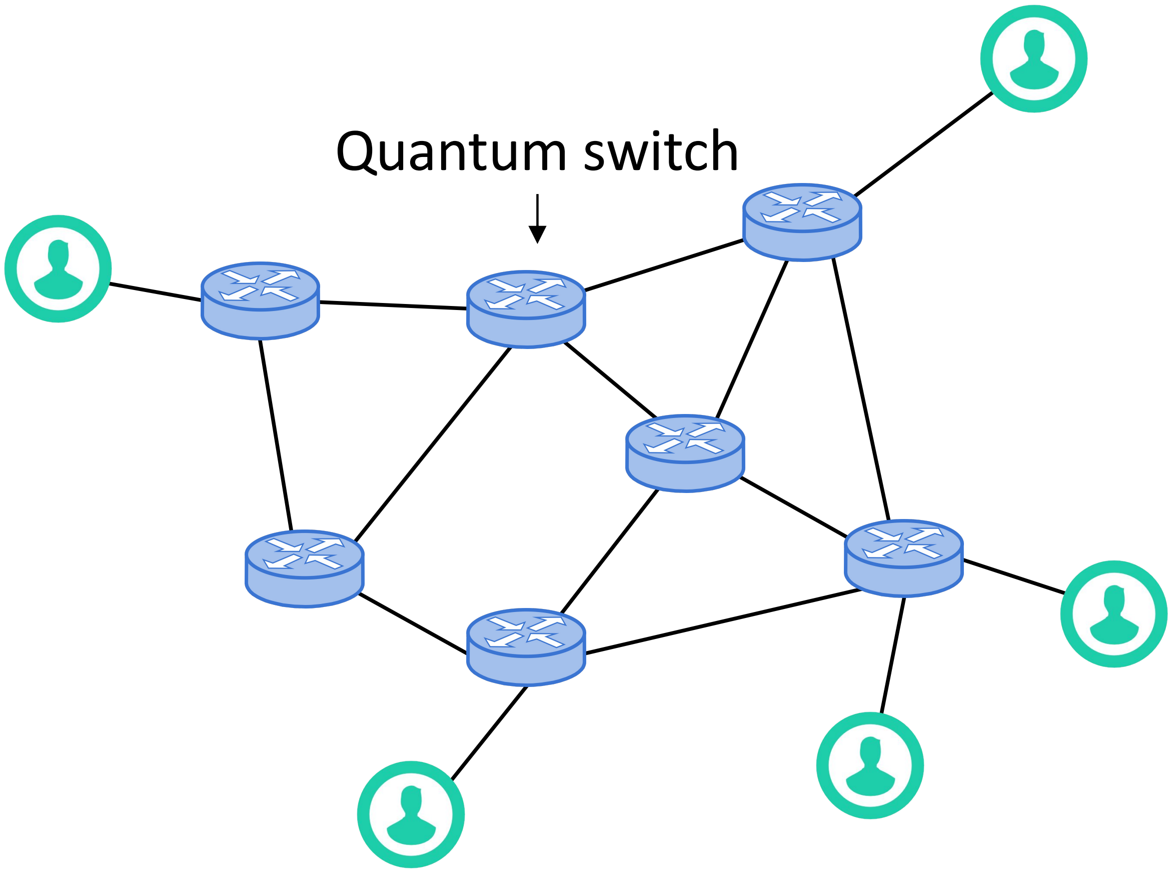
Philippe Nain

Inria Emeritus

AEP'12, Grenoble, July 4-5, 2022

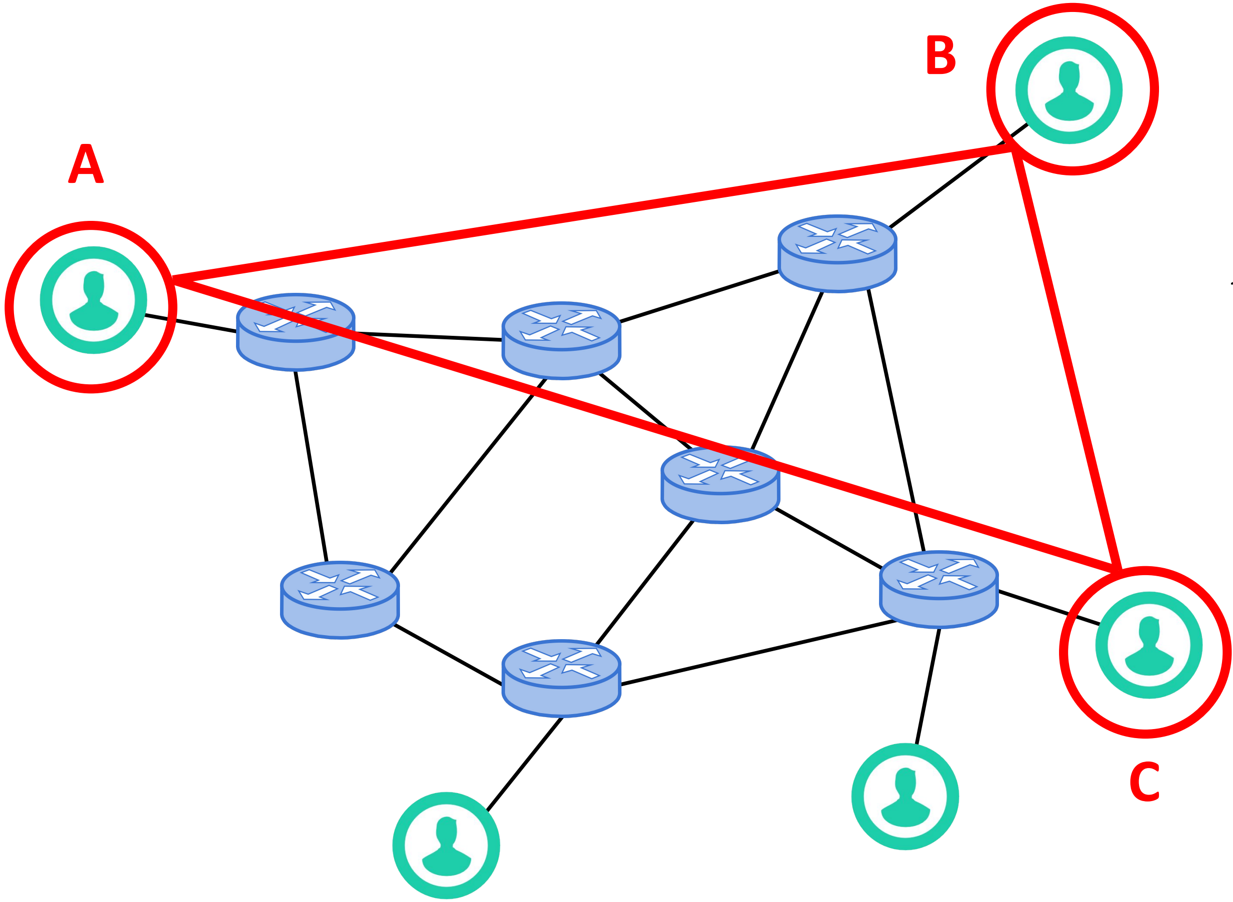
with G. Vardoyan (QuTech, TU Delft), S. Guha (Univ. Arizona, Tucson),
D. Towsley (Univ. Massachusetts, Amherst)

Quantum network



Objective: provide **entangled** states to sets of users

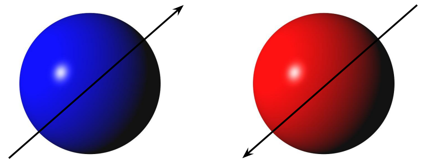
Quantum network



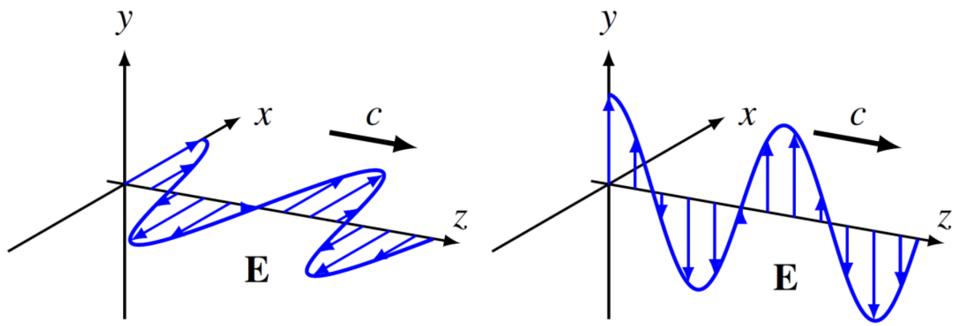
A, B, C share entangled qubits

Very short primer on entanglement

- qubit is a two-state/level mechanical system
  - spin of an electron (up, down)



  - polarization of a photon (horizontal, vertical)



Quantum bit

- classical bit is **either** 0 **or** 1
- qubit is in **superposition** of two basic states

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

α and β are complex numbers

$|\alpha|^2$= prob. of finding qubit in state 0

$|\beta|^2$= prob. of finding qubit in state 1

$$|\alpha|^2 + |\beta|^2 = 1.$$

Measurement collapse

After measurement quantum state **collapses** to either state 0 or state 1.

Quantum entanglement

Two qubits (or more) can be in **shared** state, in which operations on one affect the other(s). Qubits are said to be **entangled**.

Example: one of four **Bell pairs** is

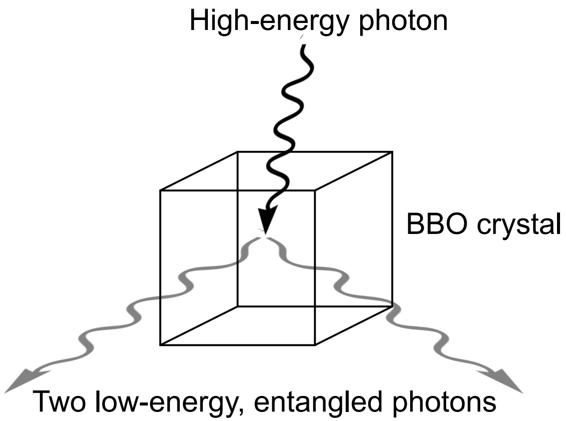
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}$$

If one qubit is measured in state i=0,1 (prob. ½) other qubit is also measured in state i.

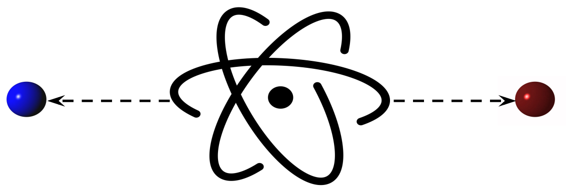
Entanglement generation

Many methods exist, some experimentally demonstrated.

- parametric down conversion (PDC)



- radioactive substance emitting electrons upon decay



Entanglement generation

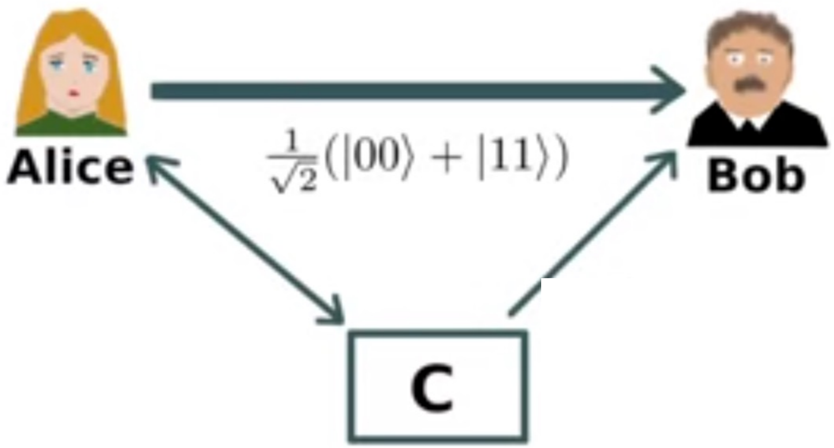
Sharing entangled state between users forms basis of much of quantum communication/computing.

Applications include

- quantum cryptography (Quantum Key Distribution or QKD)
- distributed quantum computing
- quantum sensing
- quantum machine learning.

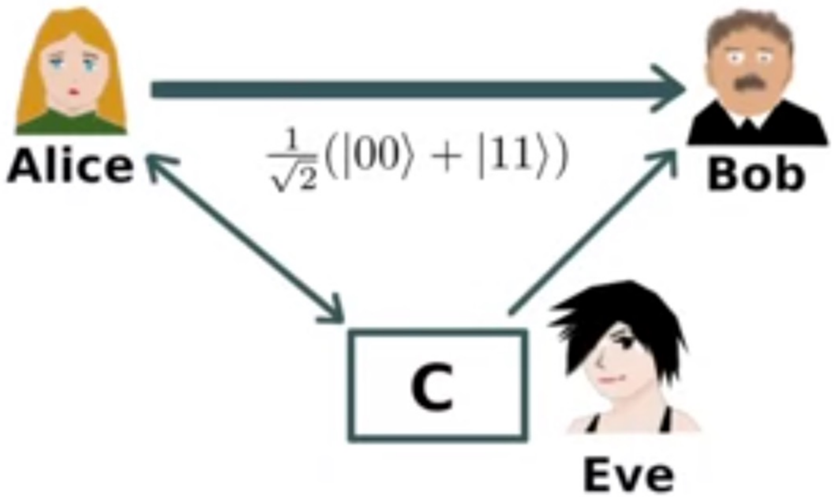
Networks must be able to create them efficiently.

E91 protocol for secret key generation



- Alice asks third party (C) to generate pairs of **entangled** photons (Bell pairs): one photon goes to Alice, other photon goes to Bob.
- When Alice and Bob measure in |0>, |1> basis they find same value i.e. 0 with prob. ½, 1 with prob. ½.
- Repeating this operation n times generates shared key with n bits.

E91 protocol for secret key generation



Key feature: Eavesdropper can be detected (Alice and Bob measure in two different basis, |0>, |1> and |+>, |->).

Artur K. Ekert « Quantum cryptography based on Bell's theorem »
Physical Review Letters 67 (6), pp. 661-663, 1991.

Secure communications

QKD enables secure communications.

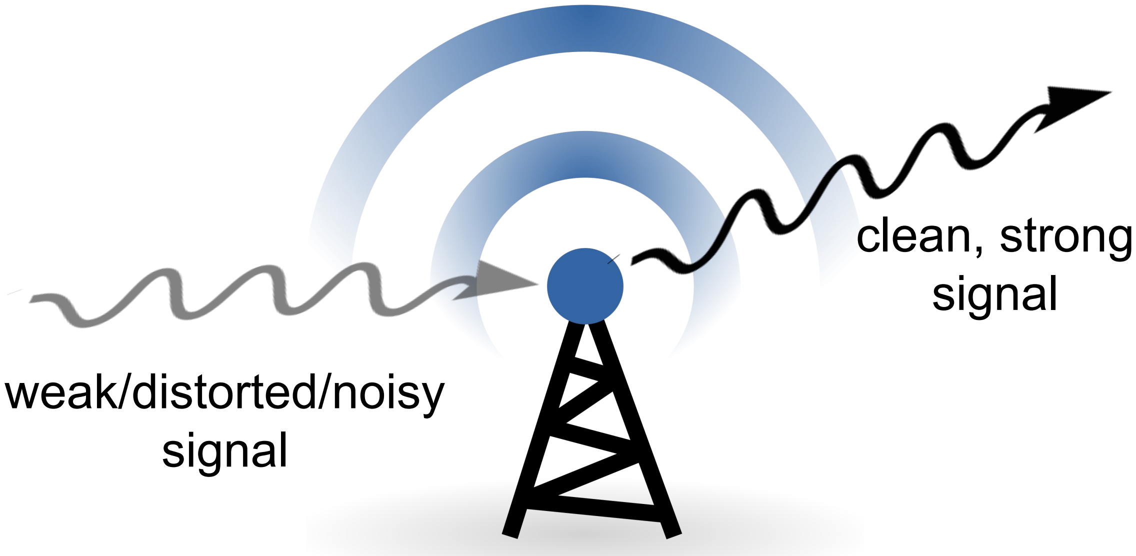
Problem

Difficult to transmit quantum state across long distance, both on optical fiber and through free space.

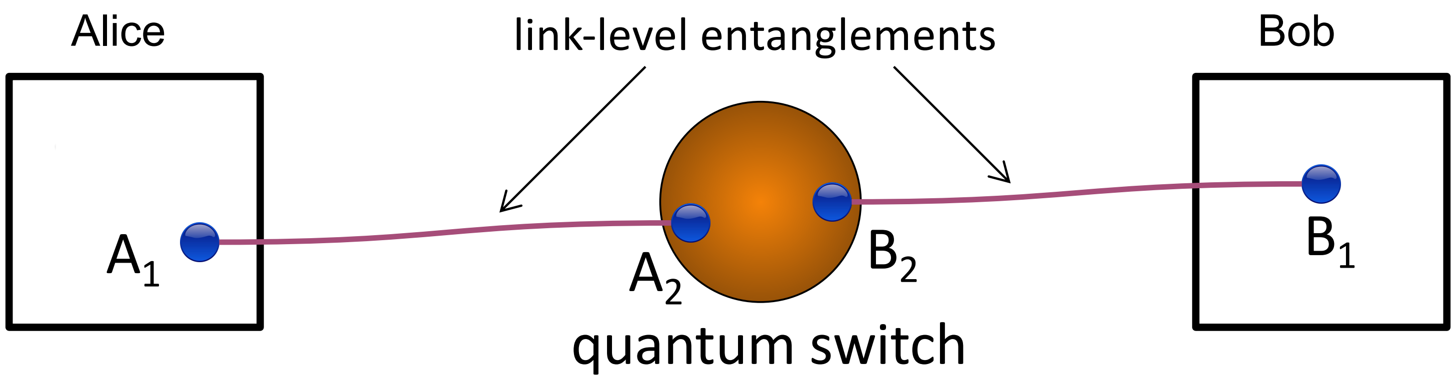
Need for **quantum switching** network supplying **end-to-end entanglement** to groups of endpoints that request them.

Need for quantum network

In classical network one can use repeaters.



Smallest quantum network: Quantum switch

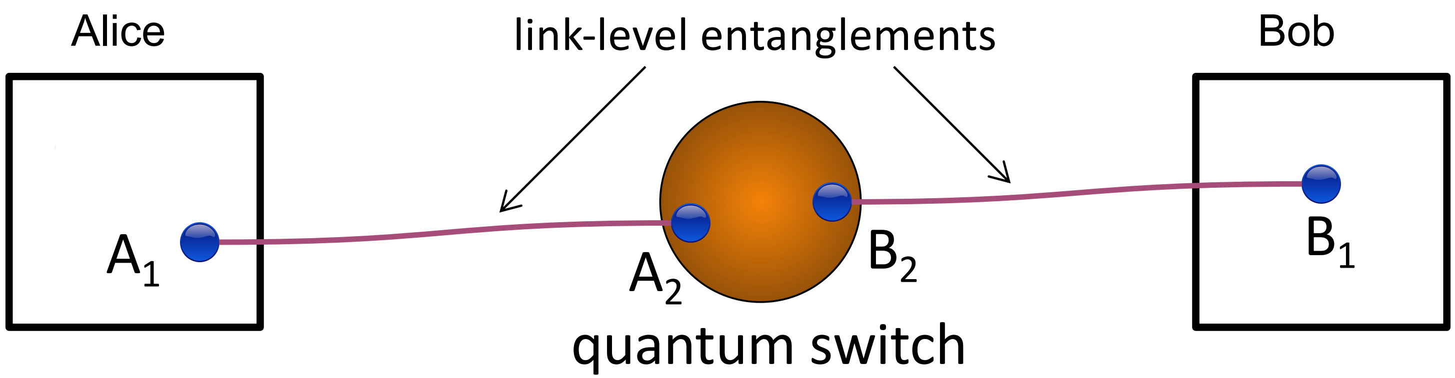


qubits A1 and A2 (resp. B1 and B2) are entangled

Goal: Entangle A_1 and B_1

Short story: this can be done!

Smallest quantum network: Quantum switch



qubits A1 and A2 (resp. B1 and B2) are entangled

Goal: Entangle A_1 and B_1

Longer story: How?… given quantum state **can neither be regenerated nor copied**.

No-cloning theorem: It is physically impossible to create copy of arbitrary unknown quantum state.

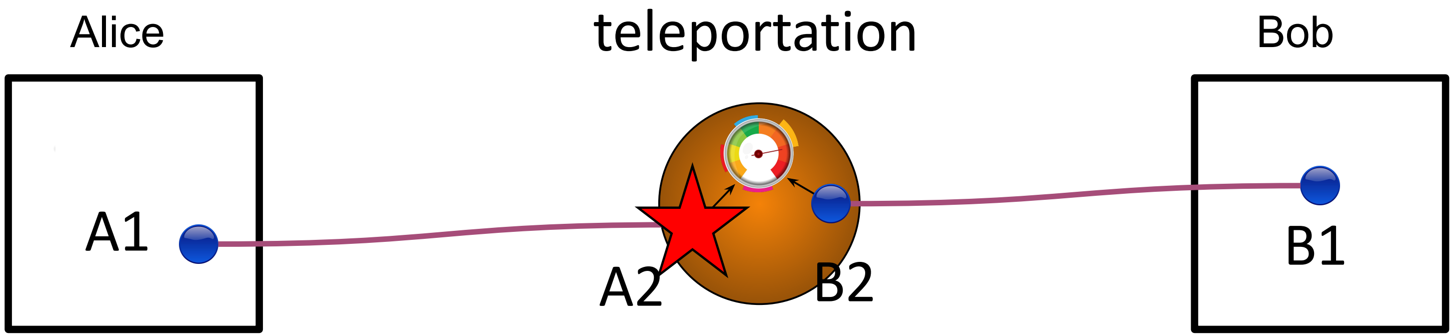
Smallest quantum network: Quantum switch

Solution

Teleportation

C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, « Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen Channels » *Physical Review Letters*, vol. *70,* pp. 1895-1899, 1993.

Smallest quantum network: Quantum switch

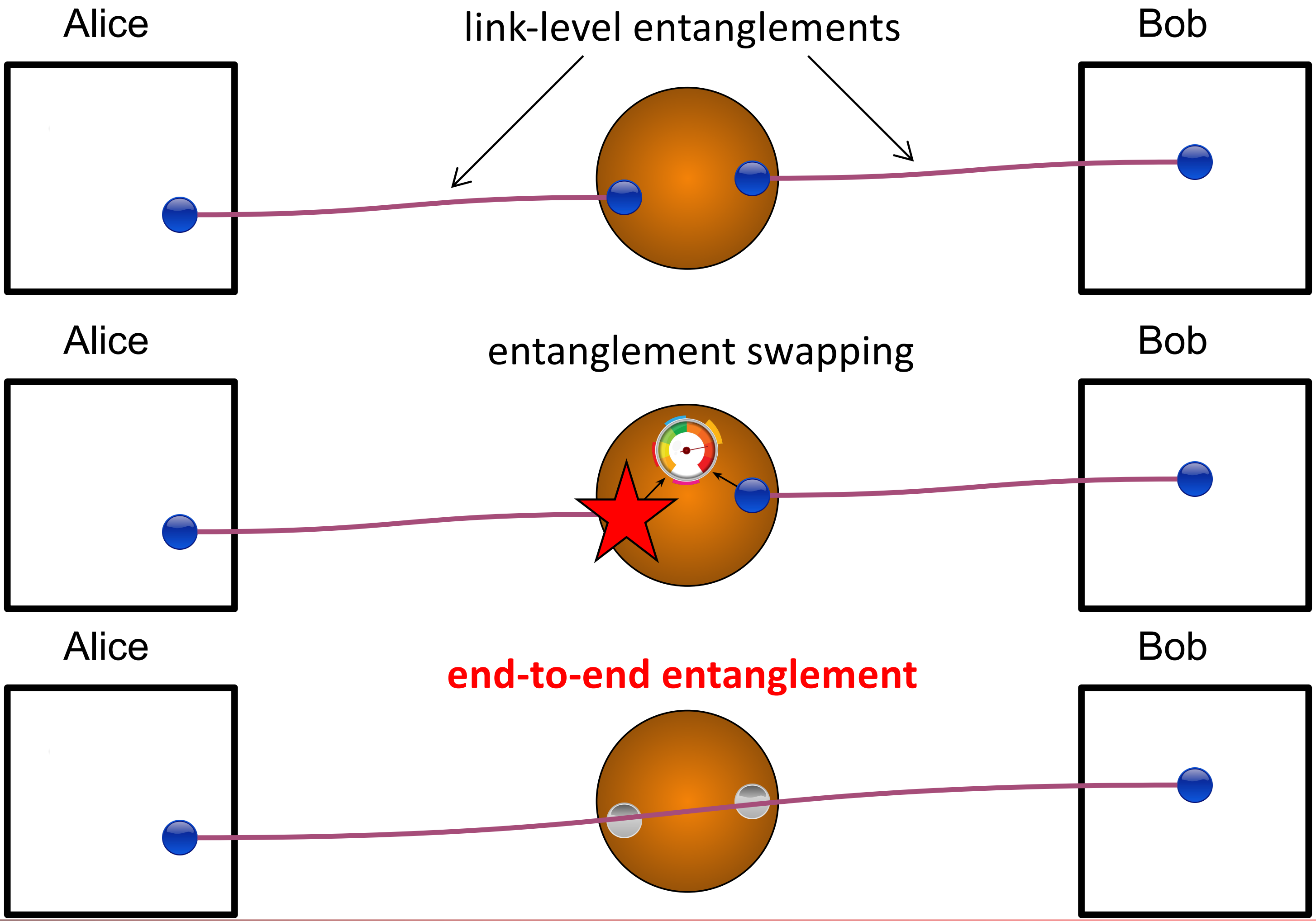


- quantum opns on qubits A_2 and B_2 (c-not and Hadamard gates) followed by measurement (whose result is (0,0) or (0,1) or (1,0) or (1,1))
- measurement result sent to Bob via **classical** medium (no faster than light!)
- with this information Bob performs quantum opns on B_1, **which then inherits quantum state** of A_2

→ qubits A_1 and B_1 are entangled (**entanglement swapping**)

- entanglement swapping may fail
- both qubits A2 and B2 collapse.

Smallest quantum network: Quantum switch

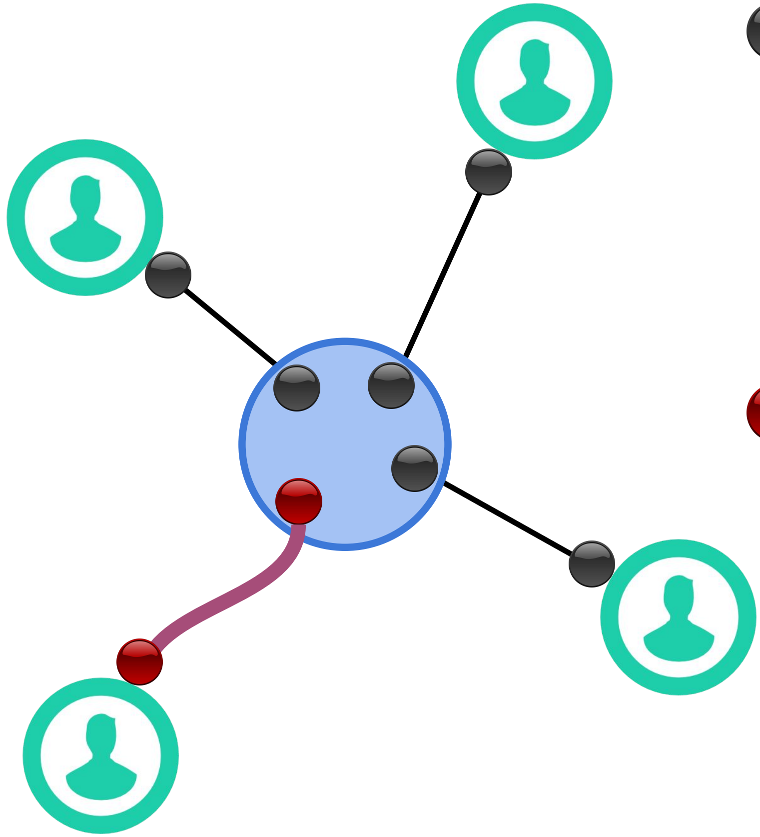


Smallest quantum network: Quantum switch

Switch equipped with quantum memories (buffers)

B quantum memories allocated to each **link**

Here B=1

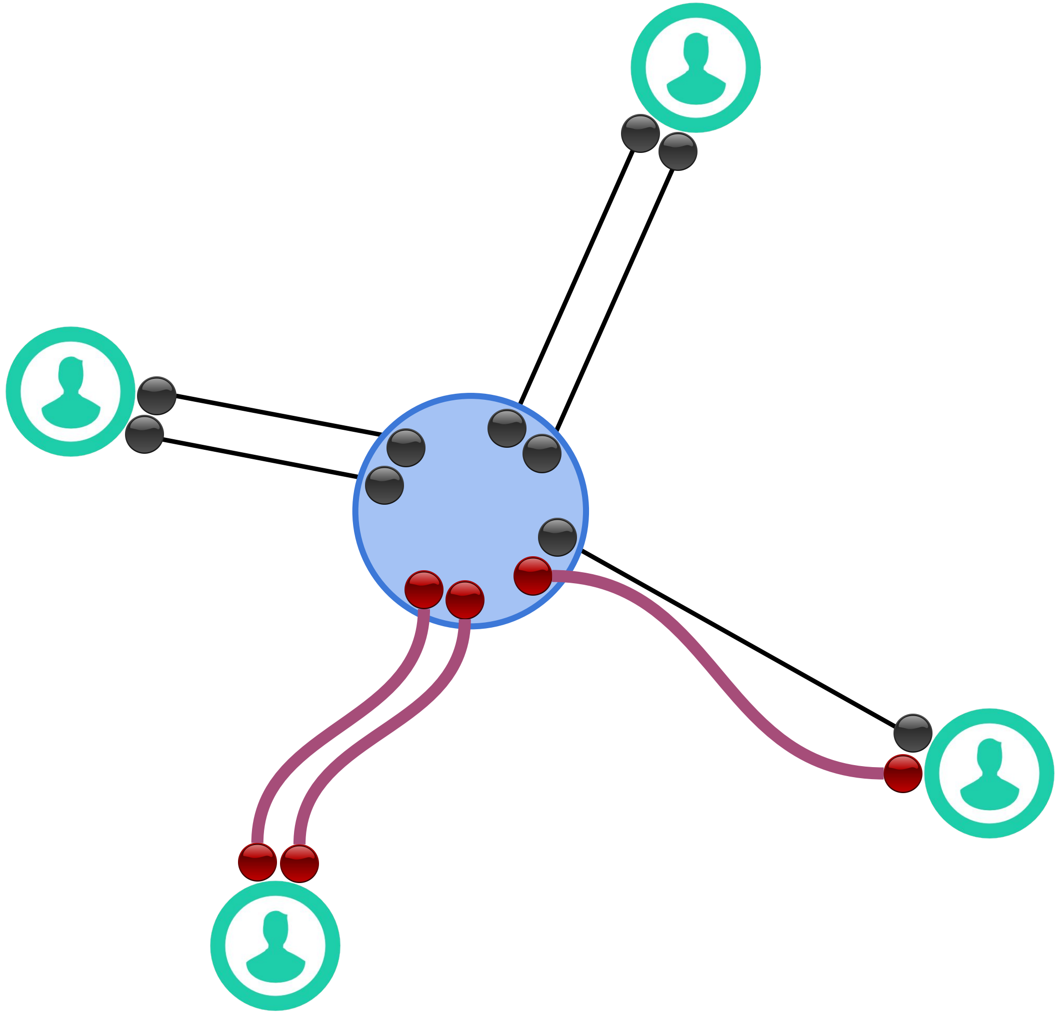


unoccupied quantum memory

occupied quantum memory

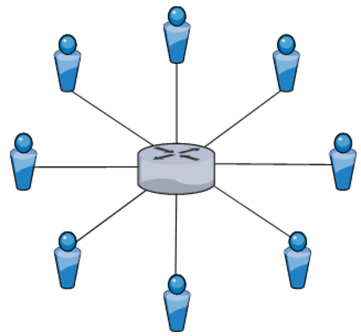
Smallest quantum network: Quantum switch

B=2



Performance of single quantum switch

Performance metrics of interest:



A quantum switch serving k users in a star topology.

- stability when B is infinite
- capacity (end-to-end entanglement rate)
- nb. available entanglements (Bell pairs).

n-partite entanglement

Case of n-partite entanglement ($2 \leq n \leq k$):
as soon as n links non-empty, swap takes place

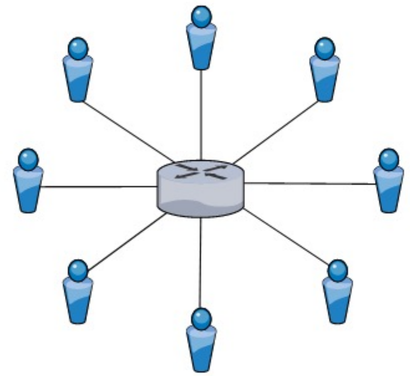
Infinite memory storage at links

Analysis for B =∞ (infinite memory at links)

- k users, k identical links
- At any time, **any combination of n users** ($2 \leq n \leq k$) wishes to share entangled qubits

➡ As soon as n distinct link-level entanglements available, **attempt** to create **n-partite** entanglement

Succeeds with prob. q



- Link-level entanglement generation is Poisson, rate μ
- Independence assumptions.

Analysis for B =∞

Property: at most n-1 links can be non-empty.

Identical links allow us to construct n-th dimensional **continuous-time** Markovian representation

$$\mathbf{x}=(x_1,\ldots, x_{n-1}) \in R_j, \quad j=0,1,..,n-1,$$

indicating nb. available entangled pairs per link, with

- $\mathbf{x} \in R_j$ if it has exactly j **zero** entries ($(0,\ldots,0) \in R_{n-1}$).

Analysis for B =∞

Uniformizing this Markov process (Poisson process with rate μk) yields DTMC **X** := {(X_1(t), …, X_{n-1}(t)), t=1,2..} with non-zero transitions

$$\mathbf{x} \in R_0 \to \begin{cases} \mathbf{x} - \mathbf{1}, & \text{with prob. } \frac{k-(n-1)}{k}, \\ \mathbf{x} + \mathbf{e}_l, & \text{with prob. } \frac{1}{k},\ l = 1, \ldots, n-1, \end{cases}$$

$$\mathbf{x} \in R_j \to \begin{cases} \mathbf{x} + \mathbf{e}_l, & \text{with prob. } \frac{k-(n-1-j)}{kj} \text{ if } x_l = 0, \\ \mathbf{x} + \mathbf{e}_l, & \text{with prob. } \frac{1}{k} \text{ if } x_l \geq 1, \end{cases}$$

$$\text{for } j = 1, \ldots, n-2,\ l = 1, \ldots, n-1, \text{ and}$$

$$\mathbf{0} \to \mathbf{e}_l \text{ with prob. } \frac{1}{n-1},\ l = 1, \ldots, n-1.$$

Reminder: **x** $\in$ R_j if it has exactly j **zero** entries.

Results for B =∞ [Sigmetrics 2020]

k = nb. users

any combination of n users wishes to share entangled qubits, $2 \le n \le k$

μ = link-level entanglement rate

q = prob. successful swapping

- System stable iff. n<k (→ unstable when n=k)
- System capacity is qμk/n
- E[total # of available Bell pairs] = k(n-1) / 2(k-n)

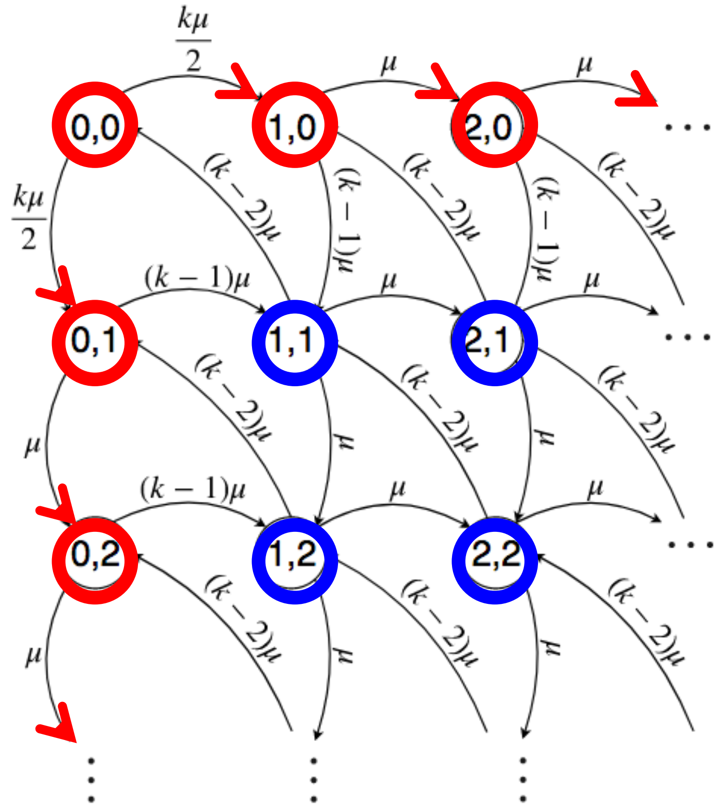
Results for B =∞ [Sig. 2020]

- System stable iff. n<k: Proof of “if part” uses Foster criterion.

Problem: **X** has infinitely many boundary states whose drift is positive regardless of choice of Lyapounov function.

Solution: Apply Foster criterion to MC embedded in **X** at times when all entries of **X** are non-zero.

n=3



Results for B =∞ [Sig. 2020]

- System capacity is $q\mu k/n$

If system stable

$$E[V(\mathbf{X}(t+1)) - V(\mathbf{X}(t))] = 0 \quad \text{for } E[V(\mathbf{X}(1))] < \infty$$

with $\mathbf{X}(t) := (X_1(t), \ldots, X_{n-1}(t))$.

Choosing $V(\mathbf{x}) = x_1 + \ldots + x_{n-1}$ yields result.

Intuition: μk = total link-level entanglement rate

➔ Successful n-partite swapping has rate $q\mu k/n$.

Results for B =∞ [Sig. 2020]

- E[total nb. available Bell pairs] = k(n-1) / 2(k-n)

This time choosing

V(**x**) = min(T, $x_1^2 + \ldots + x_{n-1}^2$) and V(**x**) = min(T^2, $(x_1 + \ldots + x_{n-1})^2$)

and letting T→∞ yields result.

Technique does not apply for variance (yields open syst. of eqns). For n=3 variance obtained in [Questa, 2022].

Bipartite entanglement (n=2)

Case of bipartite entanglement (n=2):
as soon as two links non-empty, swap takes place

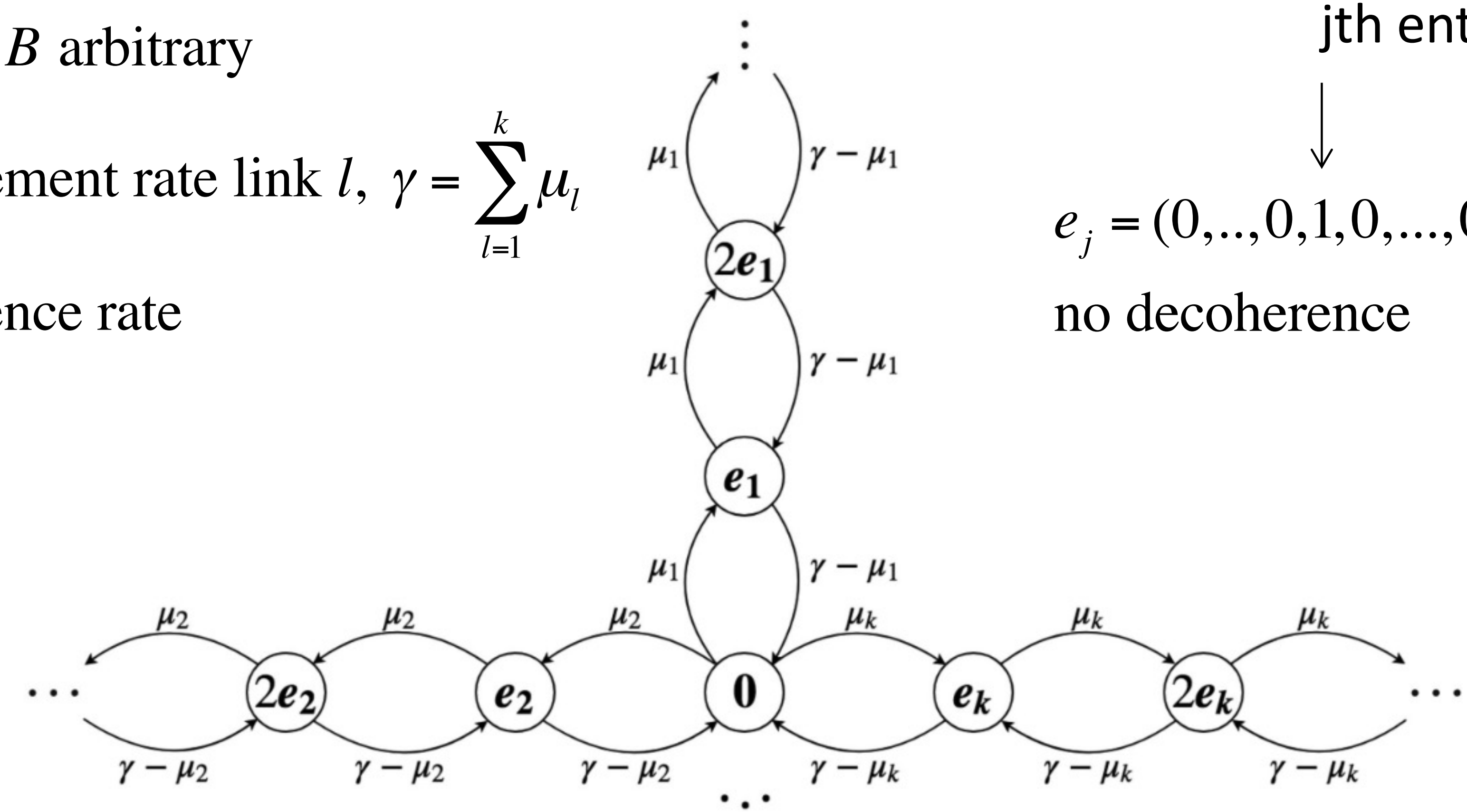
Arbitrary memory storage at links

Bipartite entanglement (n=2), heterogeneous links, decoherence

$n = 2, \;\; k > 2, \; B$ arbitrary

μ_l = entanglement rate link l, $\gamma = \sum_{l=1}^{k} \mu_l$

α = decoherence rate



jth entry

$e_j = (0,..,0,1,0,...,0)$

no decoherence

decoherence: in state je_k replace γ-μ_k by γ-$\mu_k - j\alpha$

Bipartite entangl. (n=2), heterogeneous links, decoherence

$n = 2,\ \ k > 2,\ B$ arbitrary

μ_l = entanglement rate link l, $\gamma = \sum_{l=1}^{k} \mu_l$

α = decoherence rate

Q = # available Bell pairs

$X(t) = (X_1(t),\ldots,X_k(t))$ system state time t

$X_l(t) \in \{0,1,\ldots,B\}$ # stored qubits link l

$\{X(t), t \geq 0\}$ Markov chain on $\{0,1,\ldots,B\}^k$

$\pi_0 = \lim_{t\to\infty} P(X(t)=(0,\ldots,0))$

$\pi_l^{(j)} = \lim_{t\to\infty} P(X(t)=je_l)$, j=1,…,B, l=1,…,k

The balance equations are

$$\pi_0\mu_l = \pi_l^{(1)}(\gamma - \mu_l),\, l \in \{1,\ldots,k\}$$

$$\pi_l^{(j-1)}\mu_l = \pi_l^{(j)}(\gamma - \mu_l),\, l \in \{1,\ldots,k\},\, j \in \{2,\ldots,B\}$$

$$\pi_0 + \sum_{l=1}^{k}\sum_{j=1}^{B} \pi_l^{(j)} = 1$$

and have solution (with $\rho_l := \mu_l/(\gamma\text{-}\mu_l)\ \ \forall l$)

$$\pi_l^{(j)} = \rho_l^j \pi_0,\, l \in \{1,\ldots,k\},\, j \in \{1,\ldots,B\}$$

with $\pi_0 = \left(1 + \sum_{l=1}^{k}\sum_{j=1}^{B}\prod_{i=1}^{j} \frac{\mu_l}{\gamma - \mu_l + i\alpha}\right)^{-1}$

Bipartite entanglement (n=2) [IEEE TQE 2021]

$n = 2,\ \ k > 2,\ B$ (buffer size) arbitrary, μ_l = entanglement rate link l, $\ \gamma = \sum_{l=1}^{k} \mu_l$

α = decoherence rate, Q = # available Bell pairs

$$\pi_0 = \left(1 + \sum_{l=1}^{k} \sum_{j=1}^{B} \prod_{i=1}^{j} \frac{\mu_l}{\gamma - \mu_l + i\alpha}\right)^{-1}$$

$$C = q\pi_0 \sum_{l=1}^{k} \sum_{j=1}^{B} (\gamma - \mu_l) \prod_{i=1}^{j} \frac{\mu_l}{\gamma - \mu_l + i\alpha}$$

$$E[Q] = \pi_0 \sum_{j=1}^{B} j \sum_{l=1}^{k} \prod_{i=1}^{j} \frac{\mu_l}{\gamma - \mu_l + i\alpha}.$$

Stability when B=∞:

- always stable when $\alpha > 0$
- stable when $\max_{1 \le l \le k} \mu_l < \gamma/2$ when $\alpha = 0$.

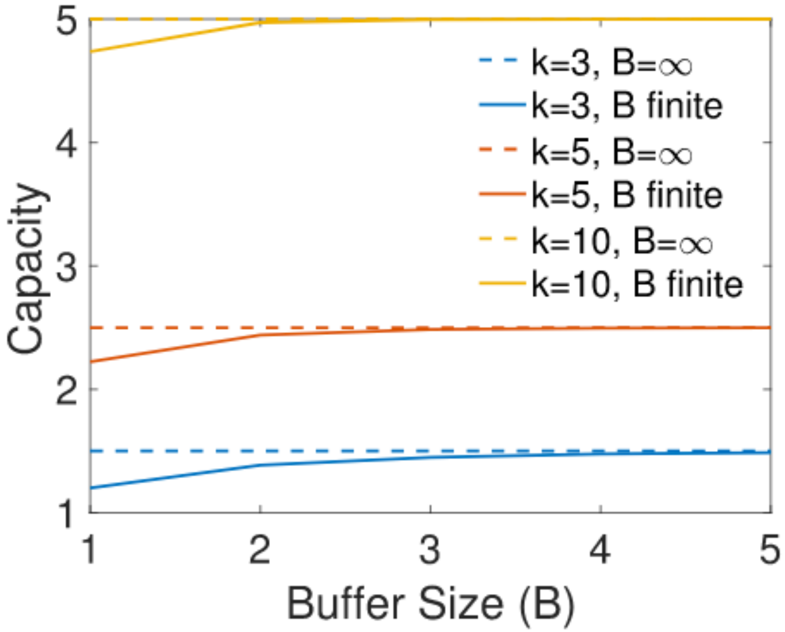
Bipartite entanglement (n=2) [IEEE TQE 2021]

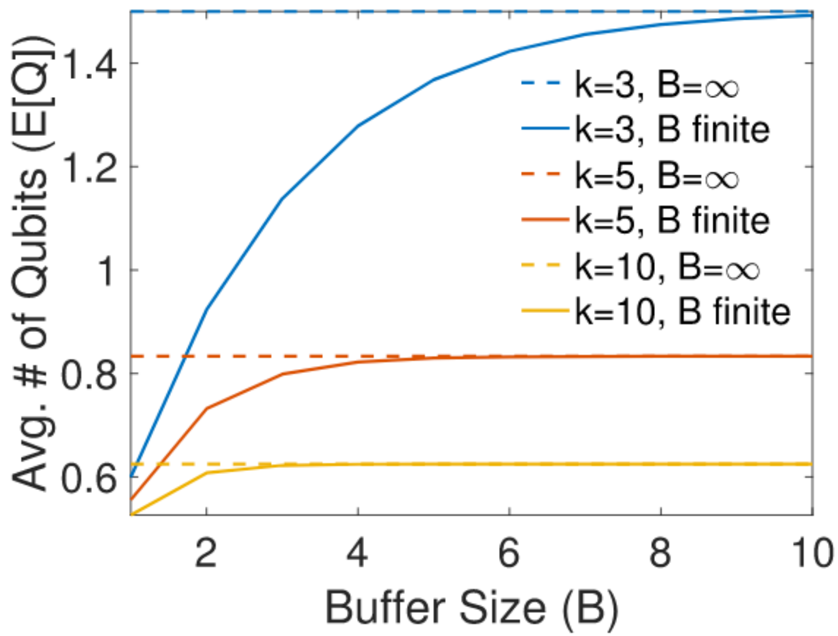
$n = 2,\ \ k > 2,\ B$ (buffer size) arbitrary

Identical links ($\mu = \mu_l,\ l = 1,\ldots,k,\ q\mu = 1$)

No decoherence ($\alpha = 0$).

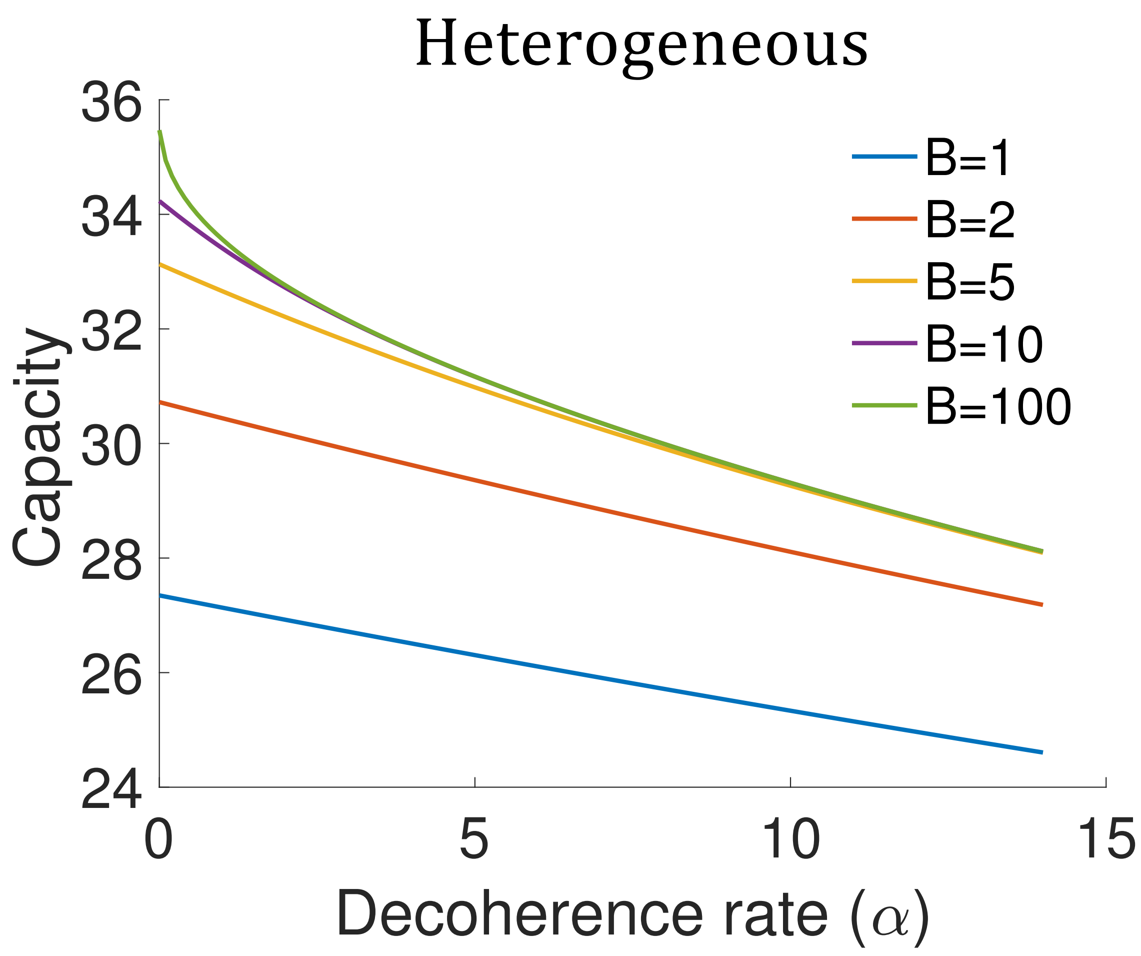
- Homogeneous system behaves as B=∞ for B≥5 (for all k>2 for C, as long as k≥5 for E[Q]).





Bipartite entanglement (n=2) [IEEE TQE 2021]

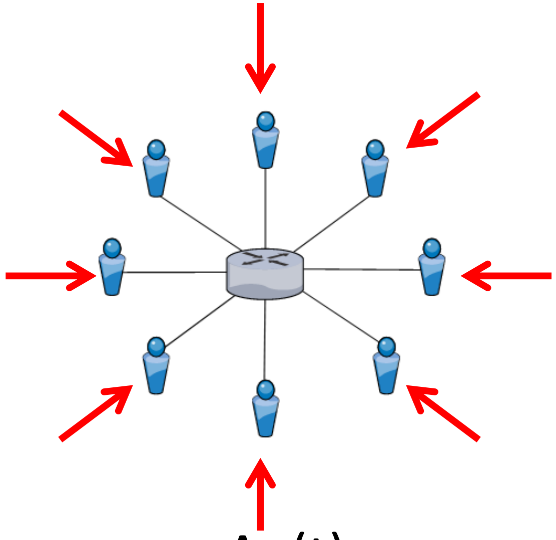
- k=5 (5 links)
- Entanglement generation rates (35, 15, 15, 3, 3), avg. 14.2 Mbits/sec.
- Homogeneous system achieves better capacity for all values of buffer size (B).



Ongoing work (with W. Dai , MIT, & D. Towsley, UMass)

Entanglement **requests** randomly arrive at users.

$A_{i,j}(t)$ = entanglement requests in slot t
between users i and j



Design protocols that schedule entanglement swapping operations in quantum switches.

Goal is to stabilize quantum switch so that number of unfinished entanglement **requests** bounded with high probability.

Research directions

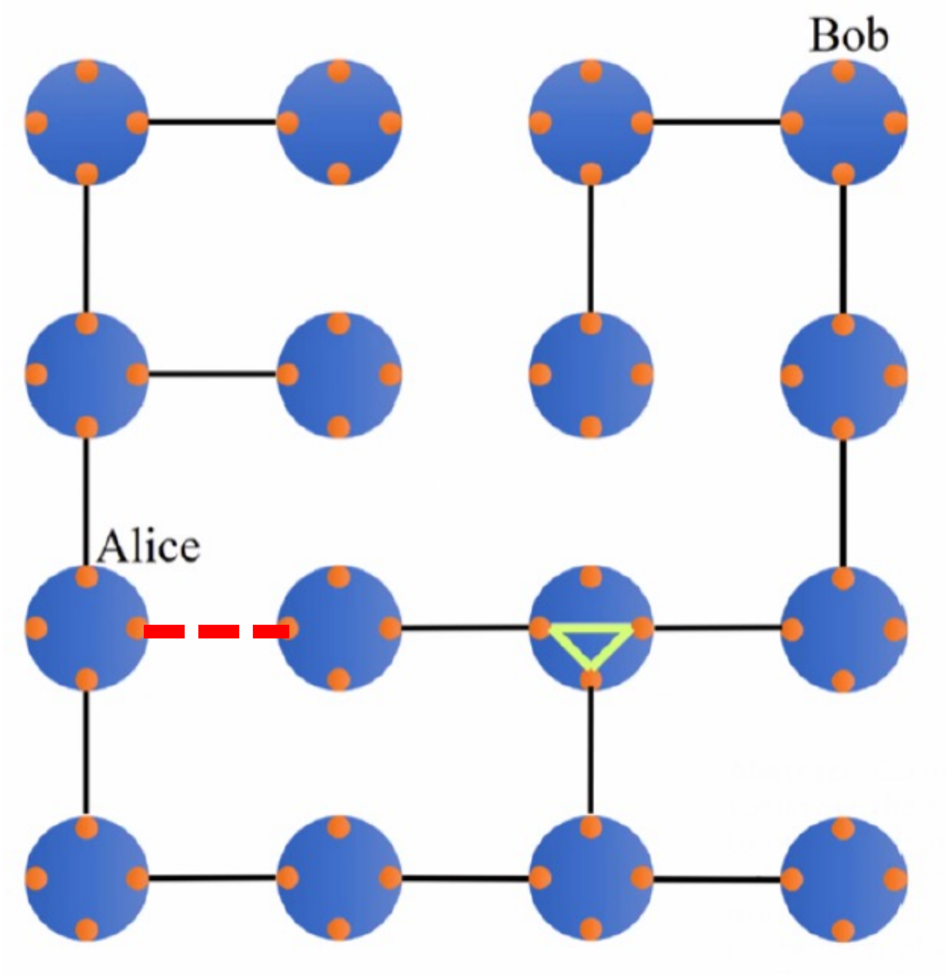
Analysis of **network** of quantum switches.

One specificity: shortest-path may not be available.

Research directions

Alice and Bob's qubits are entangled via a path that is not the shortest one.

Missing 'quantum link'



Thank you!

Q&A.

http://www-sop.inria.fr/members/Philippe.Nain/publications.html