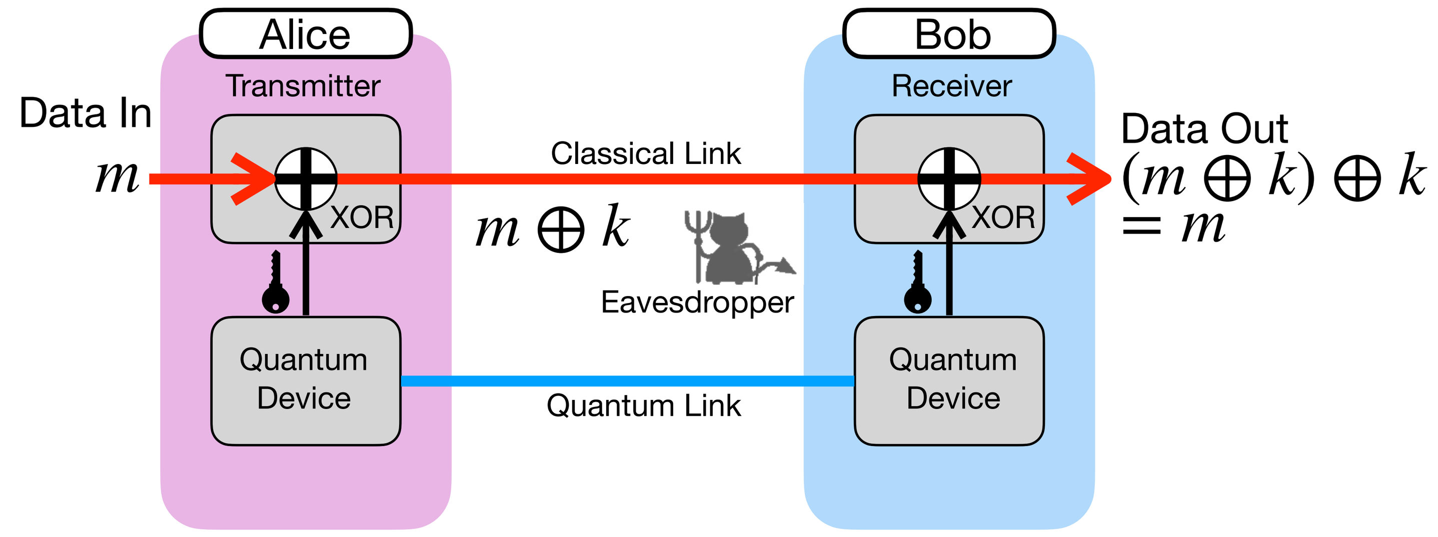
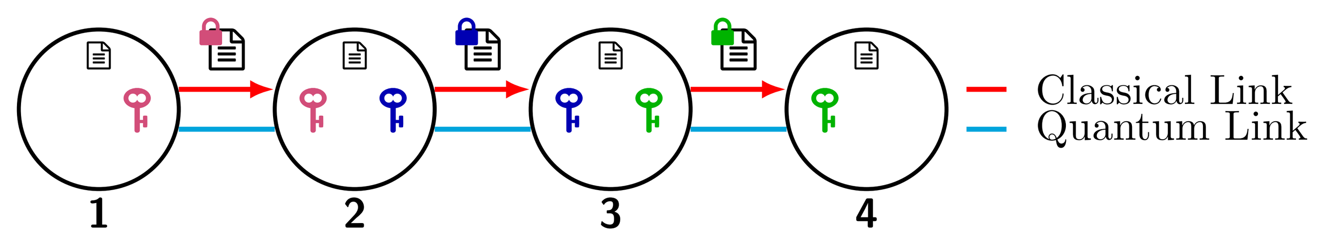
Tandem Queue Decomposition: A Throughput-Optimal Routing Policy for Quantum Key Distribution Networks

Shahbaz Akhtar*, Krishnakumar G*, Vishnu B*, Abhishek Sinha†

Introduction



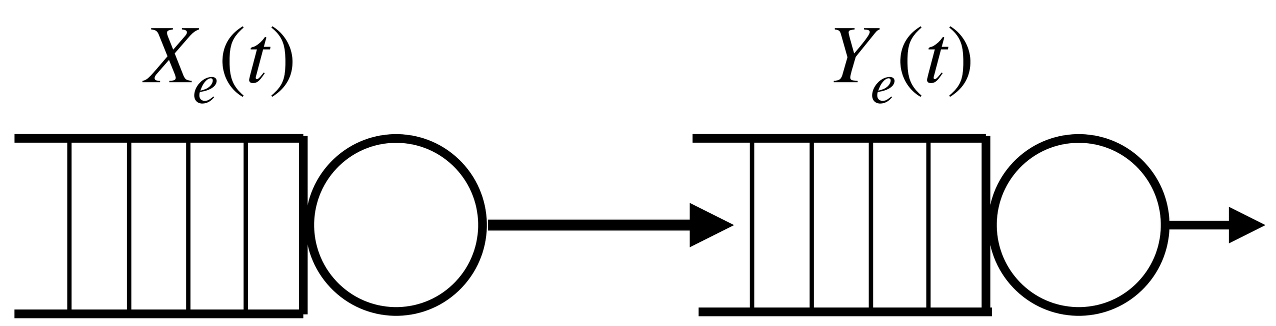
- Quantum key distribution (QKD) enables two geographically separate communicating parties to exchange symmetric private keys, whose information-theoretical security is guaranteed by the fundamental principles of quantum mechanics
- Top figure shows Alice and Bob equipped with a quantum link and classical link exchanging a sufficiently long quantum key k through quantum link to encrypt the message m that is sent over the classical link
- We consider trusted node architecture where nodes are assumed to be secure and only the links can be compromised . The architecture is shown in the figure below



Model

- We consider a network with arbitrary topology, represented by a graph $\mathcal{G}(V, E)$, where V denotes the set of nodes ($|V| = n$) and E denotes the set of edges ($|E| = m$)
- Physical link capacity is γ_e and quantum key generation rate at η_e. for edge e. Packet arrival is assumed to be i.i.d. across the time slots

Tandem Queue Decomposition



Unencrypted packets (Waiting for the keys)

Encrypted packets (Waiting due to limited link capacity)

Associate Virtual Queues $\tilde{X}_e$ and $\tilde{Y}_e$ for every X_e and Y_e

Algorithm

Tandem Queue Decomposition (TQD) Policy at slot t

Require: Graph $\mathcal{G}(V, E)$, Virtual Queue lengths $\{\tilde{X}_e(t), \tilde{Y}_e(t), \forall e \in E\}$ at the slot t

1: **(Edge-Weight Assignment)** Assign each edge $e \in E$ a weight $W_e(t) \leftarrow X_e(t) + Y_e(t)$.

2: **(Route Assignment)** For all incoming packets, compute a Min-Weight Route in the weighted graph $\mathcal{G}(V, E)$.

3: **(Key Generation)** Generate symmetric private keys for every edge $e \in E$ via QKD and store them in key banks.

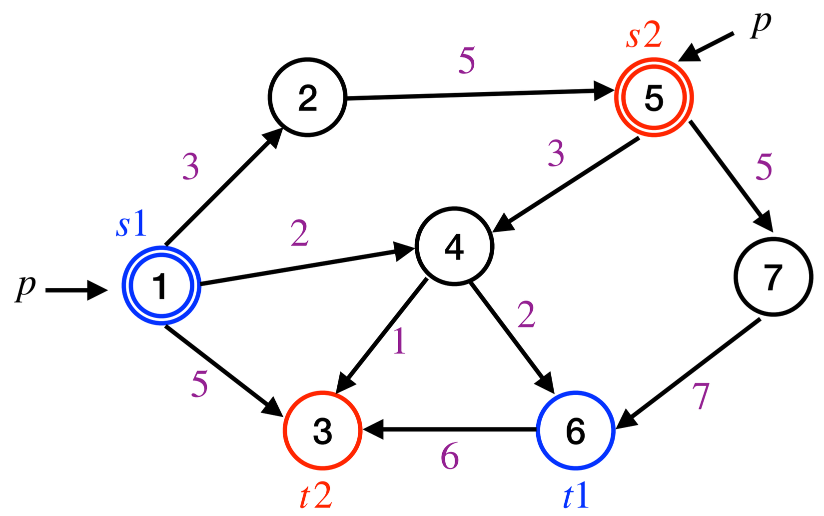
4: **(Encryption)** Encrypt the data packets waiting in the physical queue X_e with available keys in the key bank and internally transfer the encrypted packets to the downstream queue Y_e for every edge $e \in E$.

5: **(Packet Forwarding)** Forward the encrypted packets from queue Y_e to the queue $X_{e'}$ for every edge e according to some packet scheduling policy (ENTO [3] , FIFO, etc.). Here e' is the next edge in the assigned route of a packet.

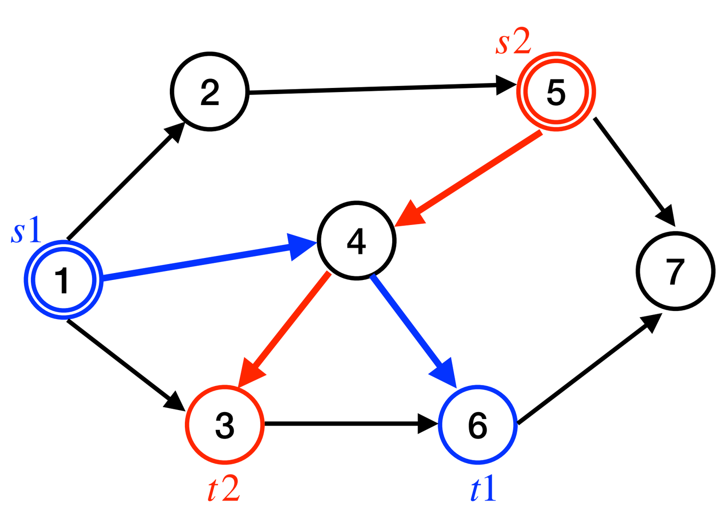
6: **(Decryption)** Decrypt the data packets received at physical queue X_e for every edge e using the symmetric key generated earlier via the QKD process.

7: **(Updating the Virtual Queues)** Update the virtual queues assuming a precedence- relaxed system, i.e.,

$$\tilde{X}_e(t+1) \leftarrow \left(\tilde{X}_e(t) + A_e^{\pi}(t) - \kappa_e(t)\right)^+, \forall e \in E$$
$$\tilde{Y}_e(t+1) \leftarrow \left(\tilde{Y}_e(t) + A_e^{\pi}(t) - \gamma_e(t)\right)^+, \forall e \in E.$$

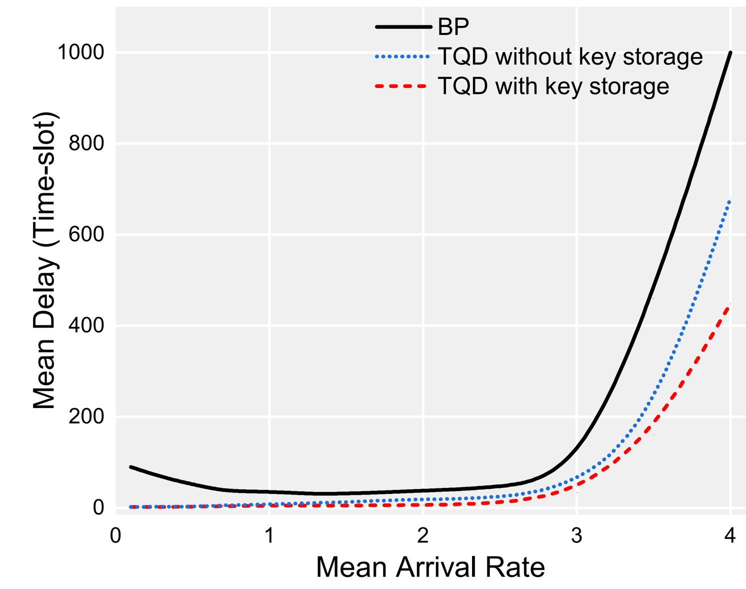


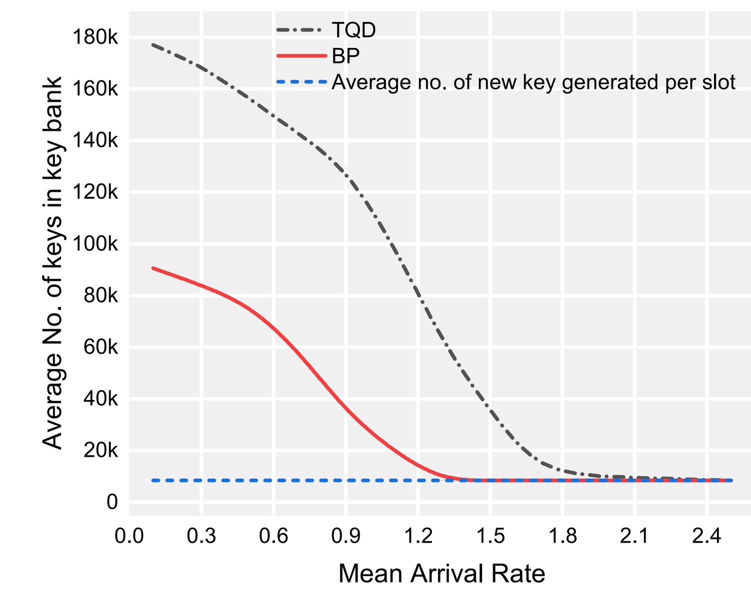
Edge-Weight Assignment



Route Assignment

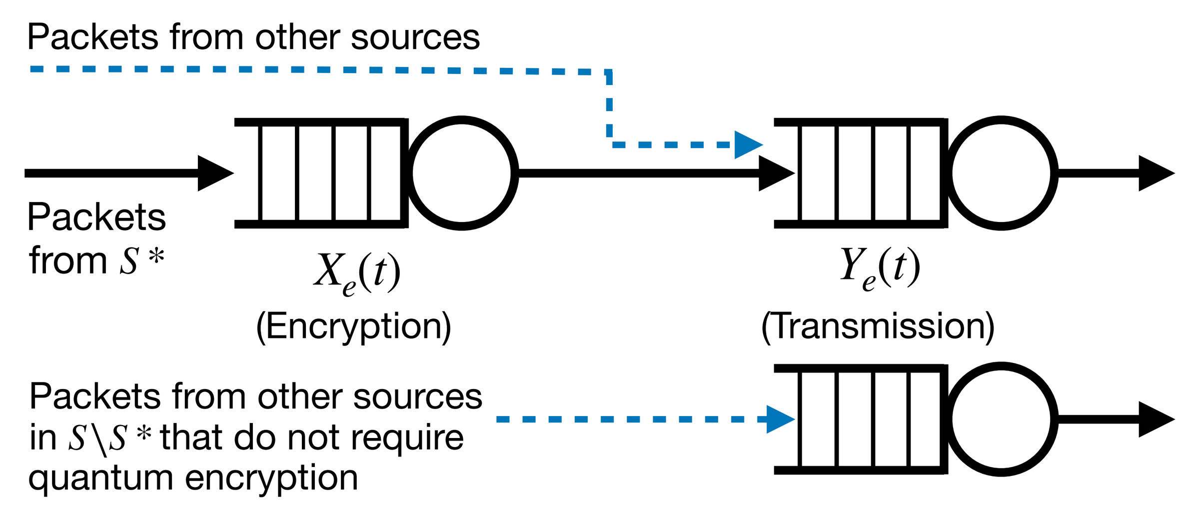
Numerical Results





- Left figure shows the variation of mean packet delay as a function of the mean arrival rate λ for unicast flow
- Backpressure performs poorly due to small congestion gradients and poor in-network residual key management at lower & higher arrival rates respectively

Extension to Multilevel Security



- Denote $S*$ to be the group of users requiring quantum encryption. In practice, some packets $S \backslash S*$ might not require quantum encryption. Those skip the X_e and join the Y_e queues directly
- $E_S \subseteq E$ be the set of edges equipped with the QKD module. The shortest path is computed on the induced graph $\mathcal{G}(V, E_S)$ for packets originating from some source in the set $S*$
- Packets from other sources are routed along the edges that lack QKD module. We call this extension to be e-TQD

References

- Vishnu B and Abhishek Sinha. Fast and secure routing algorithms for quantum key distribution networks. *In 2022 14th International Conference on COMmunication Systems NETworkS (COMSNETS)*
- Abhishek Sinha and Eytan Modiano. Optimal Control for generalized Network Flow Problems. *IEEE/ACM Transactions on Networking* 2018.
- David Gamarnik. Stability of adaptive and non-adaptive packet routing policies in adversarial queueing networks. *In proceedings of 31st annual ACM symposium on Theory of Computing* 1999.

*Indian Institute of Technology Madras, †Tata Institute of Fundamental Research