Efficient optimization of secret-key rates in quantum repeater chains

Tim Coopmans[1], Boxi Li[2], Sebastiaan Brand[3], David Elkouss[1]

[1]QuTech, Delft University of Technology, The Netherlands, [2]Eidgenössische Technische Hochschule Zürich, Switzerland, [3]Leiden Institute of Advanced Computer Science, Leiden University, The Netherlands.

Click for the full articles: 2005.04946 and 1912.07688 (arxiv) [JSAC 2020]

E-mail: t.j.coopmans – at – tudelft.nl

Quantum repeaters enable surpassing the fundamental distance limit that quantum key distribution schemes can cover. However, realistic hardware parameter make their realization a challenge. In this work:

1. We provide an efficient algorithm for completely characterizing the behavior of a large class of repeater chain protocols composed of probabilistic components, improving upon the exponential runtime of existing algorithms

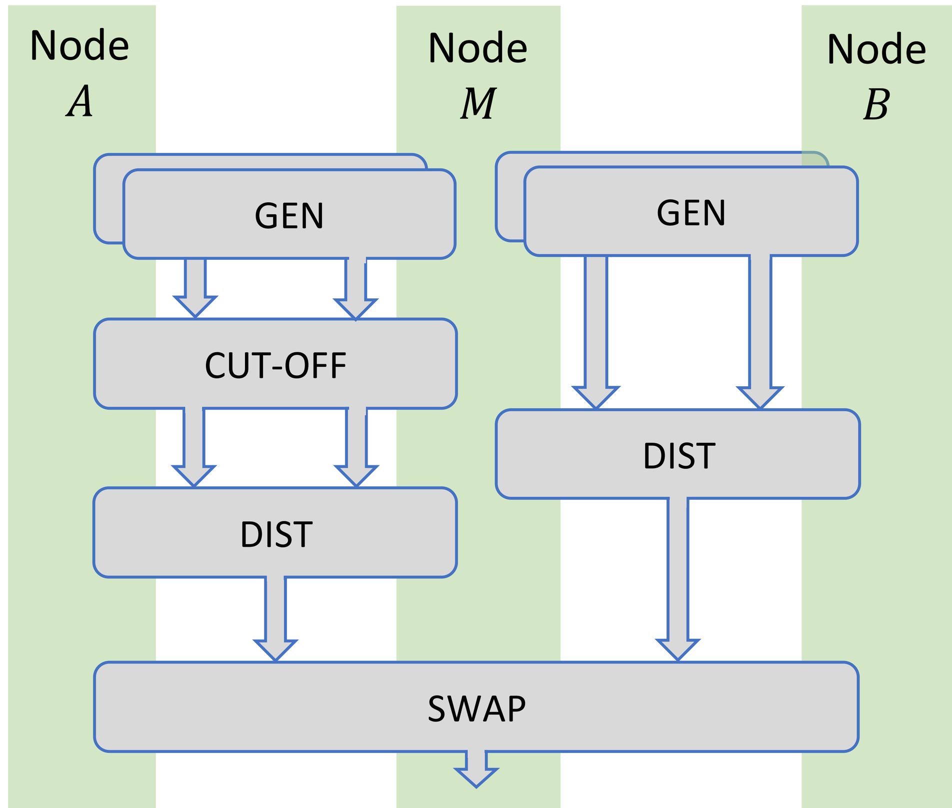
2. We use the algorithm for optimizing the available secret key rates for these schemes, which include a cut-off condition that mitigates the effect of memory decoherence. We find that the use of the optimal cut-off lowers the parameter threshold for which secret key can be generated.

Our algorithms thus serve as useful tools for the design and realization of long-distance quantum key distribution networks.

Context

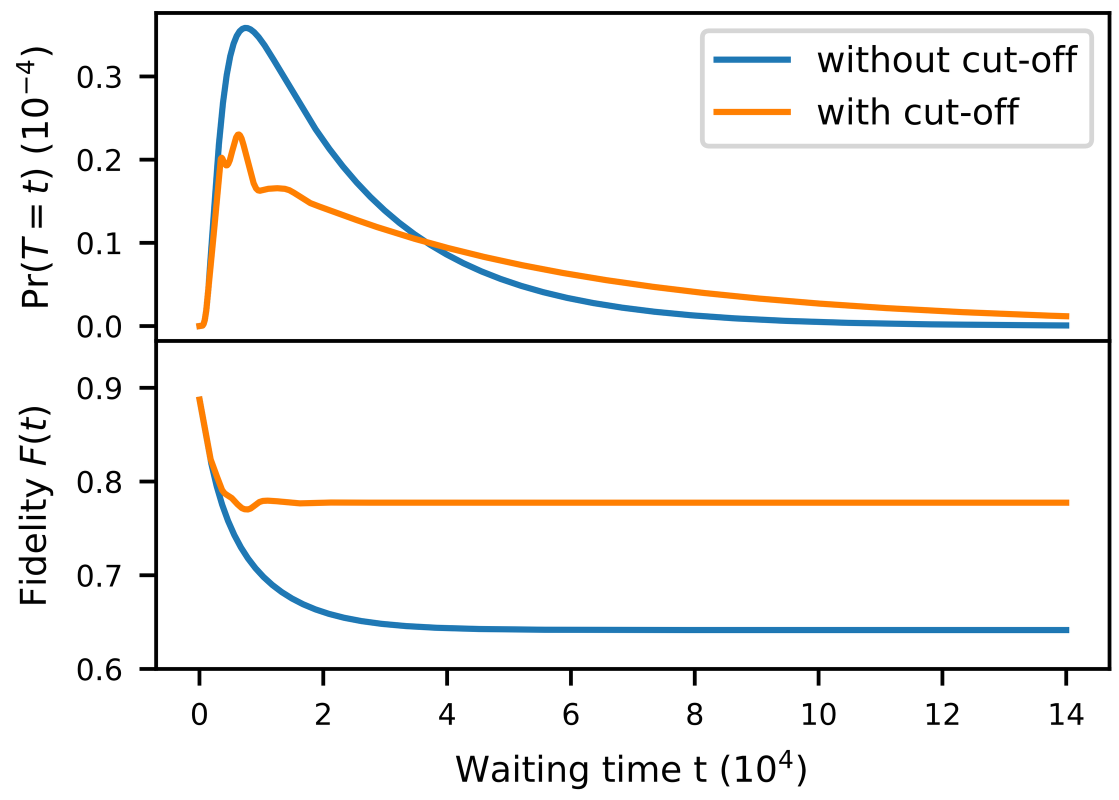
- We consider hierarchical repeater chain schemes (based on the BDCZ scheme [1]), which are composed of probabilistic components (GENeration of fresh entanglement, DISTillation, SWAPping).
- Such schemes suffer from memory decoherence which decrease state quality: many times, an entangled pair is generated which needs to wait for another pair, and decoheres during this waiting. For this reason, we also include cut-offs, where entanglement is discarded if its storage time exceeds a prespecified threshold duration.

Example scheme on 3 nodes (single arrow per entangled pair):



Our solution: efficient algorithm

- For a given composite repeater protocol, we derive closed-form expressions for the probability that a state is produced at time *t*
- These can be numerically evaluated in polynomial time in the distribution's support size cap, improving upon exponential-runtime existing algorithms for swap&cut-off schemes, based on Markov chains [2,3]
- We also extend our algorithm to include the average fidelity of the state, while keeping polynomial runtime.



Example algorithm output for 9-node repeater chain scheme of the form GEN → (CUT-OFF → SWAP)^3

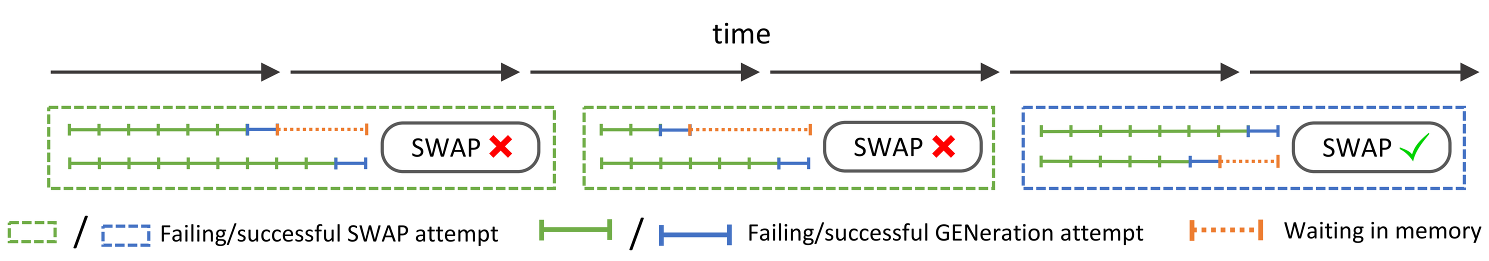
Used success probabilities: 0.001 (GEN), 0.5 (SWAP), GEN-fidelity: 0.985, coherence time 40.000 time steps). Cut-offs for the three nesting levels 1700, 3200, 5500

Problem statement

Given a repeater chain scheme, find the probability distribution of the waiting time and fidelity of the state generated between the end nodes

The time until the first end-end entangled pair is produced is random.

Example: single repeater (2 x GEN + SWAP)



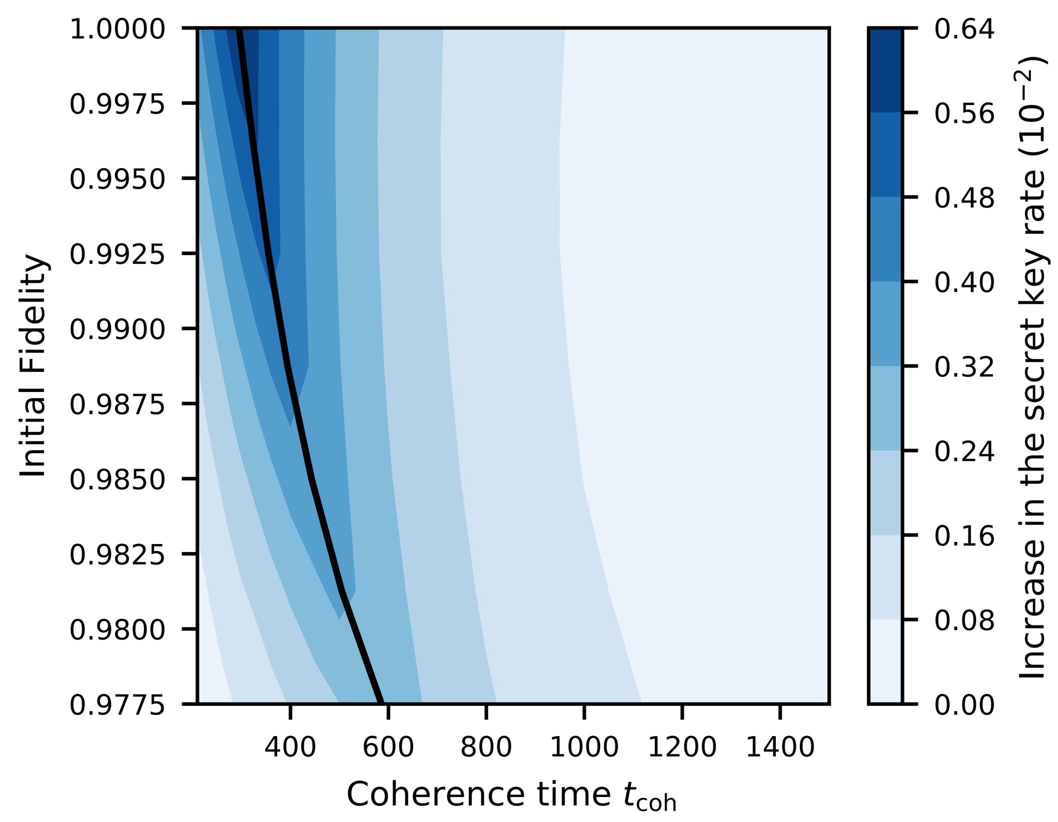
Waiting time until successful swap:

$$\sum_{\{k=1\}}^{\#swaps} \max(\text{2 copies of GENeration waiting time})$$

Since swap is probabilistic, #swaps is also a random variable!

For a general repeater scheme, the joint random variable (waiting time, fidelity of final state) can be expressed recursively by iterating over the repeater scheme's individual components (GEN, SWAP, DIST, CUT-OFF). Finding their probability distribution is a complex problem in general: e.g. #distillation-attempts is correlated to fidelity, which depends on waiting time because of memory decoherence.

Application: optimize cut-off to maximize secret-key rate



Fidelity increase of the use of the optimal-cut-offs compared to the no-cut-of alternative,. Solid line separates the area where the no-cut-off protocol produces no secret key (left of line) and where its secret- key rate is >0 (right of line).

Plotted is 9-node repeater chain scheme of the form GEN → (CUT-OFF → SWAP)^3 Used success probabilities: 0.1 (GEN) and 0.5 (SWAP)

Results:

- key generation possible with worse hardware than if no cut-off used
- higher rates than possible without (optimal) cut-off

[1] H.-J. Briegel, W. Du ̈r, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. 81, 5932–5935 (1998)
[2] E. Shchukin, F. Schmidt, and P. van Loock, Phys. Rev. A 100, 032,322 (2019)
[3] S. E. Vinay and P. Kok, Phys. Rev. A 99, 042,313 (2019).

This work was supported by the QIA project (funded by European Union's Horizon 2020, Grant Agreement No. 820445) and by the Netherlands Organization for Scientific Research (NWO/OCW), as part of the Quantum Software Consortium program (project number 024.003.037 / 3368). Boxi Li is supported by the IDEA League student grant programme.

QUANTUM INTERNET ALLIANCE

Quantum Software Consortium

IDEA League