SPONSORED BY THE Federal Ministry of Education and Research

Quantum repeaters and quantum key distribution: the role of quantum error correcting codes

S. Bratzik, H. Kampermann, and D. Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

Introduction

- Standard quantum key distribution (QKD) is limited to about 250 km due to losses in the optical fiber.
- Quantum repeaters [Bri1998] permit to extend this distance by nested entanglement distillation and entanglement swapping.
- The secret key rate (bits per memory per second) resulting from a quantum repeater is given by

$$K = \frac{R\, r_\infty}{M}, \tag{1}$$

where
  - R (repeater rate) is the average number of generated entangled pairs per second,
  - r_∞ is the secret fraction, i.e., the ratio of the secret bits and the measured bits in the asymptotic limit (Devetak-Winter bound $1 - S(X|E) - H(X|Y)$),
  - M is half the number of used memories per repeater node.
- We investigate the quantum repeater with encoding [Jia2009] in the context of quantum key distribution and compare it to the quantum repeater using distillation, as the former does not require classical communication.

Generic quantum repeater

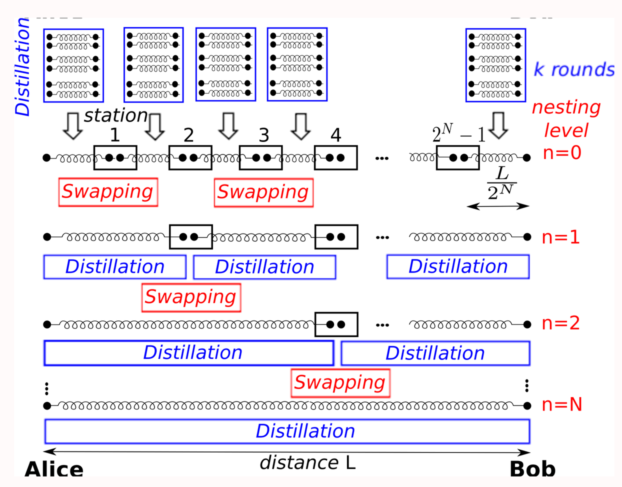

Fig. 1: A generic quantum repeater protocol [Bri1998] with maximal nesting level N and k rounds of distillation in all nesting levels.

- Problem: classical communication is needed for acknowledging the success of entanglement distribution, distillation and swapping.

Quantum repeater with encoding

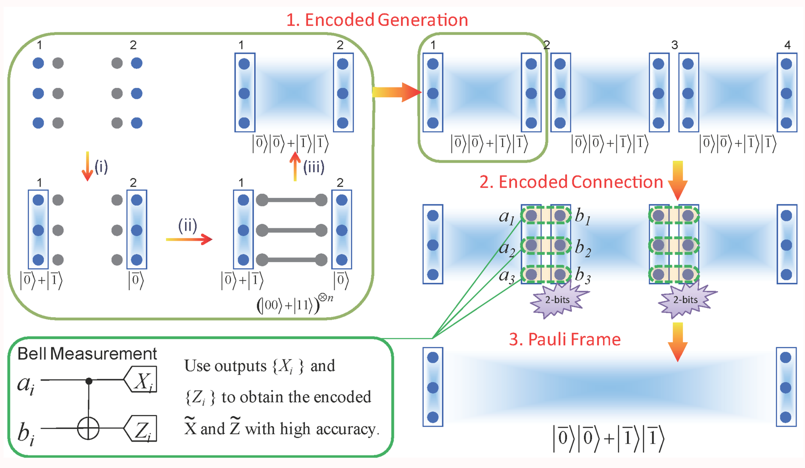

Fig. 2: Repeater protocol with encoding, from [Jia2009].

- Advantage: classical communication is only needed for acknowledging the success of entanglement entanglement distribution and in the end for communicating the Pauli frame.
- Disadvantage: many logical gates are needed.

QR with encoding: remote CNOT and error models

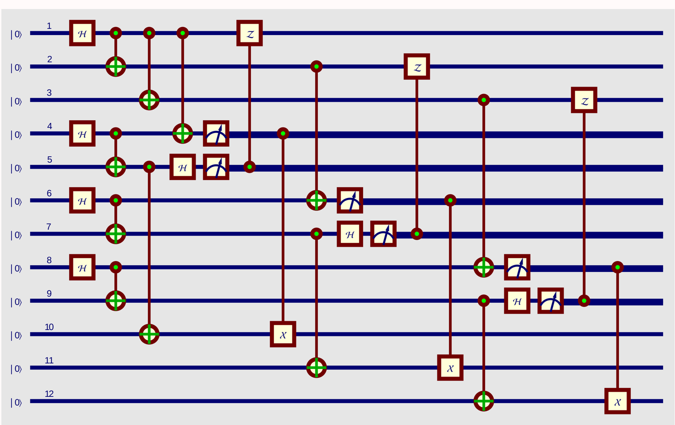

Fig. 3: Remote CNOT for the quantum repeater with encoding, adapted from [Jia2007].

Assumptions:

- One-qubit operations are error free,
- error model for two-qubit operations (depolarizing map): $O^{real}\rho = p_G O^{ideal}\rho + \frac{1-p_G}{4}\mathbb{1}$,
- Bell pairs are depolarized:

$$\rho_{Dep}(F_0) := F_0\Pi_{|\phi^+\rangle} + \frac{1-F_0}{3}\left(\Pi_{|\phi^-\rangle} + \Pi_{|\psi^+\rangle} + \Pi_{|\psi^-\rangle}\right).$$

- Application of multiple two-qubit gates and neglecting errors of order $\beta^2 = (1-p_G)^2$ and higher leads to

$$(1-\mathrm{Length}[op](1-p_G))\bigotimes_{j=1}^{\mathrm{Length}[op]} op[[j]]\rho\left(\bigotimes_{j=1}^{\mathrm{Length}[op]} op[[j]]\right)^\dagger + (1-p_G)\left\{\sum_{i=1}^{\mathrm{Length}[op]}\bigotimes_{j=1}^{i-1} op[[j]] f\left(i,\rho,\bigotimes_{j=i+1}^{\mathrm{Length}[op]} op[[j]]\right)\left(\bigotimes_{j=1}^{i-1} op[[j]]\right)^\dagger\right\},$$

where $op = \{U_m, ..., U_1\}$ is the list of gates and $f(i,\rho,A) := \mathrm{tr}_i\left(A\rho A^\dagger\right)\otimes\frac{\mathbf{1}_i}{4}$.

The repeater rate

- Average number of attempts to connect m pairs, each generated with probability P_0 ($P_0 = 10^{-\alpha L_0/10}$ is the probability that a photon is not absorbed at a distance $L_0 = L/m$) and deterministic entanglement swapping [Ber2011]:

$$Z_m(P_0) := \sum_{j=1}^{m}\binom{m}{j}\frac{(-1)^{j+1}}{1-(1-P_0)^j}. \tag{2}$$

Generic Quantum Repeater

- The repeater rate including the classical communication time can be found in [Bra2013].
- Using distillation and no classical communication time the rate is [Abr2013]:

$$R_{\mathrm{Rep}} = \frac{1}{2T_0}\left(\frac{2}{3}\right)^{N+\sum_n k_n} P_0\prod_{n=1}^{N} P_{ES}(n)\prod_{i=0}^{k_n} P_D^{\mathrm{O}}(i,n), \tag{3}$$

Quantum repeater with encoding

- For deterministic swapping:

$$R_{\mathrm{QEC}} = \frac{1}{T_0 Z_{nm}(P_0)}, \tag{4}$$

with n being number of physical qubits to encode one logical qubit.

$P_D^{\mathrm{O}}(i,n)$ is the success probability in the i-th distillation round and n-th nesting level for the *Oxford* protocol [Deu1996], $T_0 = L_0/c$ (c is the speed of light in the optical fiber), and $P_{ES}(n)$ is the success probability of entanglement swapping in the n-th nesting level.

Memories

Quantum repeater with distillation:

- Number of needed memories depend on the distillation protocol:
  - recursive protocol (*Oxford protocol* [Deu1996]): $M_O = 2^{\sum_i k_i}$,
  - entanglement pumping (*Innsbruck protocol* [Due1999]): $M_I = N + 2 - |\{k_i : k_i = 0\}|$.

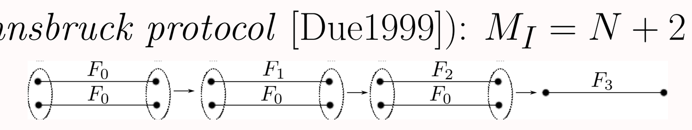

Fig. 4: Entanglement pumping (*Dür et al.* protocol [Due1999]) with $k = 3$ rounds of purification.

- For optimality of the distillation protocols and strategies see [Bra2013].

Quantum repeater with encoding

- Number of memories used here is $M_{enc} = 2n$ (overhead for the remote CNOT).

Results: optimal repeater protocol

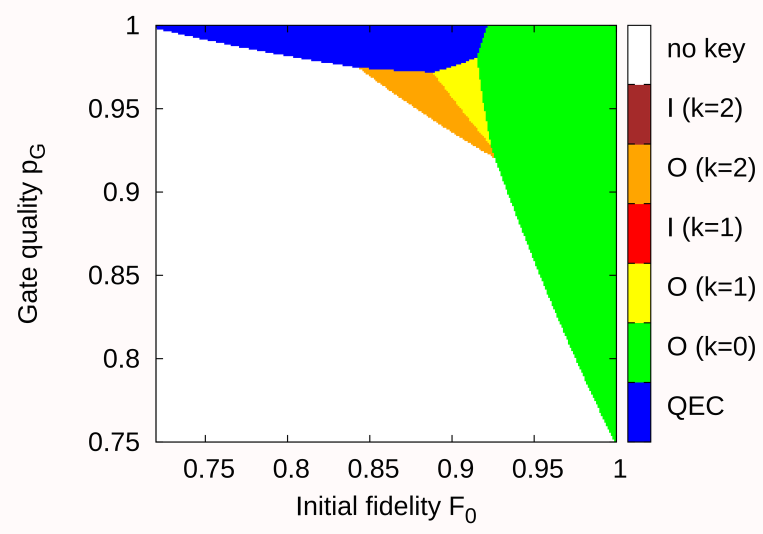

Fig. 5: Optimal quantum repeater protocols w.r.t. the secret key rate per memory per second for $N = 1$ in terms of the initial fidelity F_0 and the gate quality p_G.

- Here: distillation only in the end ($\vec{k} = \{0, k\}$) with protocols *Oxford* (O) and *Innsbruck* (I); quantum repeater with encoding (QEC) for the three-qubit repetition code ($n = 3$).
- The number of generated Bell pairs is kept the same, in case of the QEC it is 3, for distillation either 2 (for $k = 1$) or 4 (for $k = 2$).
- The total distance is $L = 600$ km.
- For initial fidelities $F_0 \leq 0.85$ the QEC is optimal.
- For an initial fidelity above $F_0 = 0.92$, no distillation is optimal.
- The *Innsbruck protocol* is not optimal for this set of parameters, but it was shown in [Bra2013] that this can be achieved for other parameters.

Results: optimal secret key rate

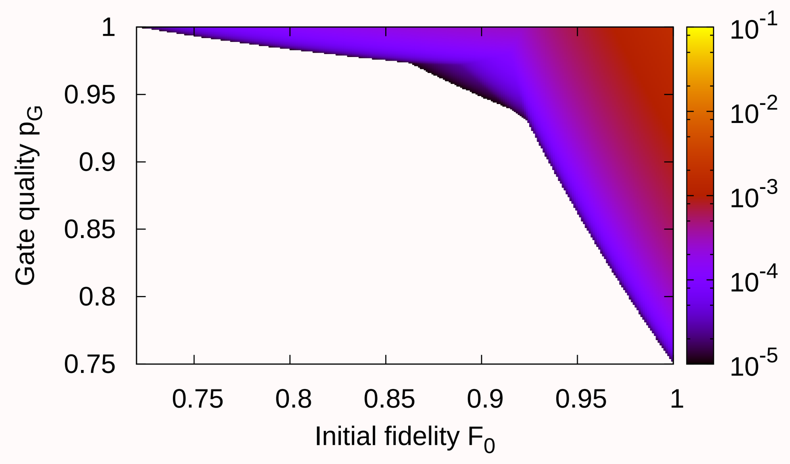

Fig. 6: Optimal secret key rate per memory per second for the quantum repeater protocols ($N = 1$) shown above in terms of the initial fidelity F_0 and the gate quality p_G.

- The generation of a non-zero secret key rate for $N = 1$ at a distance of $L = 600$ km is limited to very good gates and good initial fidelities.
- For having good gates ($p_G \geq 0.98$), but modest fidelities ($F_0 \leq 0.8$), we can still obtain a secret key rate per memory per second on the order of 10^{-4}.

Discussion

- We calculated the secret key rate per memory per second by comparing two approaches for the quantum repeater: either using distillation or using quantum error correction.
- We found that for modest fidelities ($F_0 \leq 0.8$) we can still obtain a non-zero secret key rate, but we require good gates ($p_G \geq 0.98$).
- Future work includes the extension of these calculations to higher nesting levels (more swappings) and other error correcting codes.

Acknowledgments

We thank S. Abruzzo, M. Epping, and L. Jiang for fruitful discussions. The authors acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, project QuOReP).

References

[Abr2013] S. Abruzzo, S. Bratzik *et al.*, Phys. Rev. A **87**, 052315 (2013).
[Ber2011] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).
[Bra2013] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **87**, 062335 (2013).
[Bri1998] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[Deu1996] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).
[Due1999] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[Jia2007] L. Jiang, J. Taylor, A. Sørensen, and M. D. Lukin, Phys. Rev. A **76**, 062323 (2007).
[Jia2009] L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009).