Confidentiality of the hashing protocol and applications to the quantum repeater

A. Pirker, M. Zwerger, V. Dunjko, W. Dür, H. J. Briegel

24.08.2017

Entanglement Distillation Protocols (EDP)

Entanglement distillation protocols are used to distill a maximally entangled state, e.g. a perfect Bell-pair $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, from several noisy copies via local operations and classical communication.

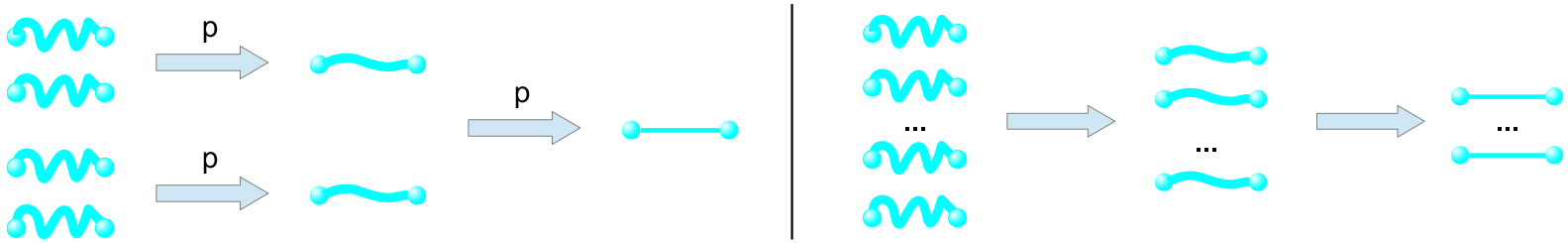

Figure: The left figure illustrates recurrence-type protocols, e.g. [1, 2] whereas the right figure depicts hashing protocols [3].

Hashing Protocol

The hashing protocol [3] is an entanglement distillation protocol that

- operates on an asymptotic large ensemble of n i.i.d. Bell-pairs
- assumes that each initial state is a two qubit density operator ρ diagonal in the Bell-basis
- outputs deterministically a fraction $m = n(1 - S(\rho))$ of systems in the $|\phi^+\rangle$ state in the asymptotic limit of n

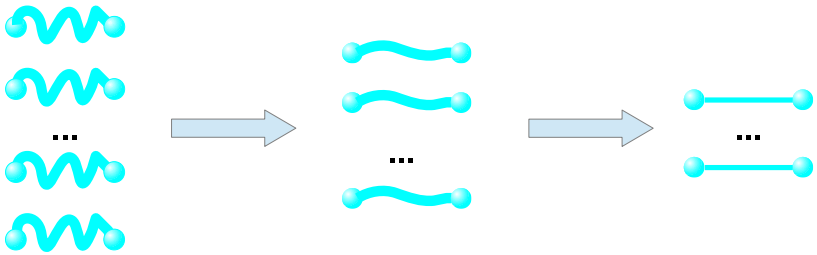

Figure: One round of hashing operates on the whole ensemble via local operations and classical communication.

Noisy measurement-based hashing

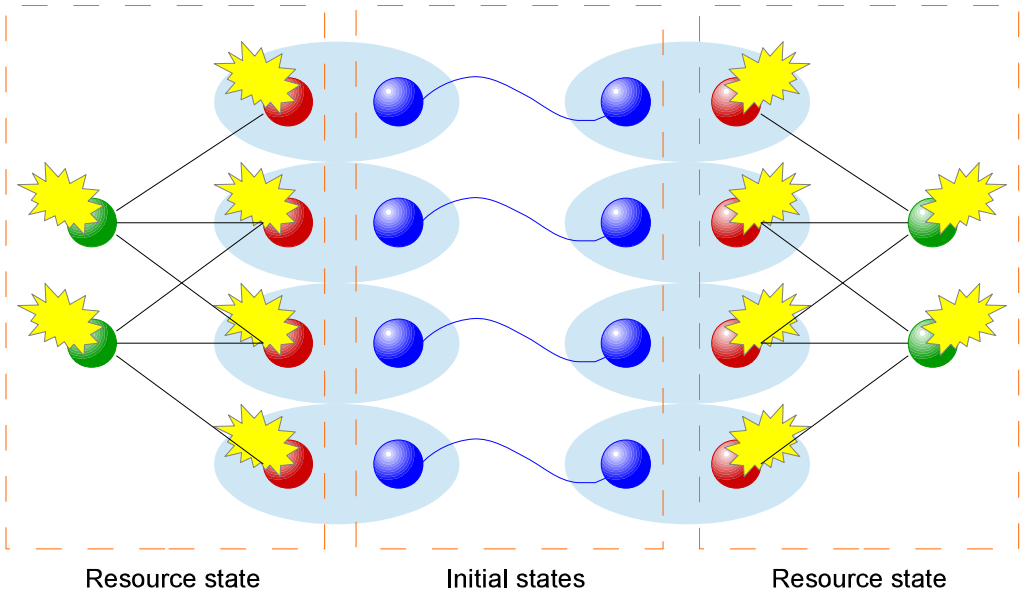

Figure: If there is noise, gate-based hashing fails ⇒ use measurement-based hashing [4]. The red vertexs correspond to input qubits whereas green vertexs to the output qubits of the resource state. We assume that local depolarizing noise (LDN) acts on those qubits identical and independent. Ellipsis indicate Bell-measurements.

Security model and overall protocol

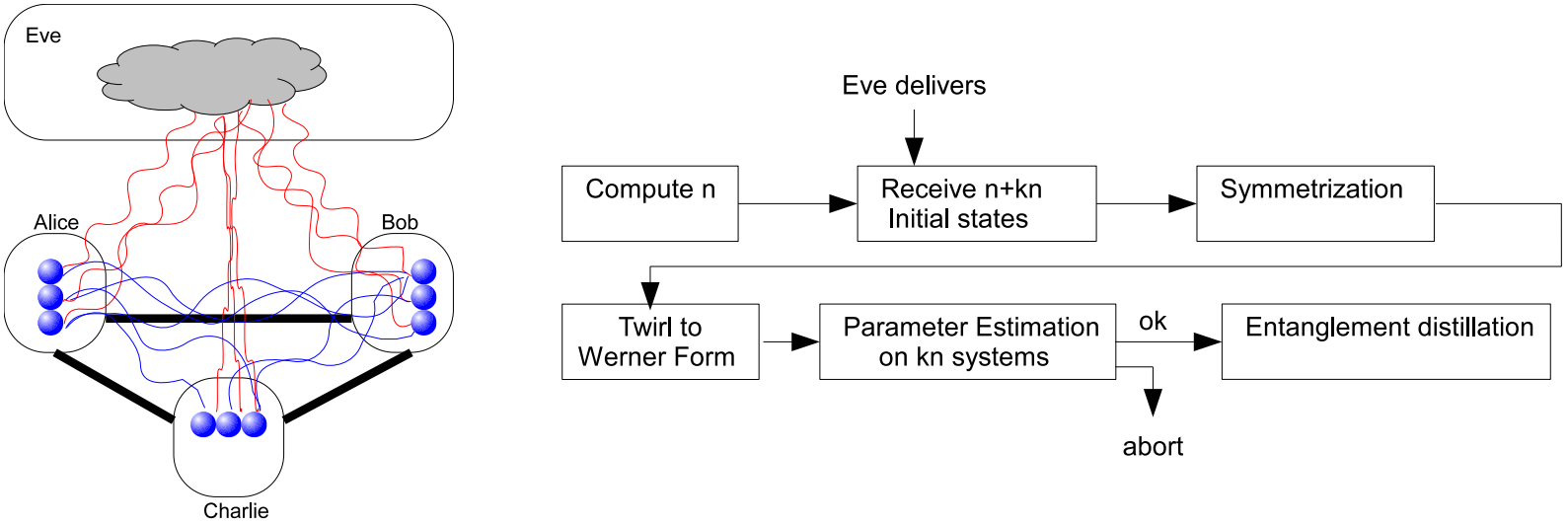

Figure: Left: Eve distributes the initial states via a noisy quantum channel to the participants. All participants are connected via classical authenticated channels. Right: Proposed overall protocol

The ideal map $\mathcal{F}$ and the confidentiality criterion

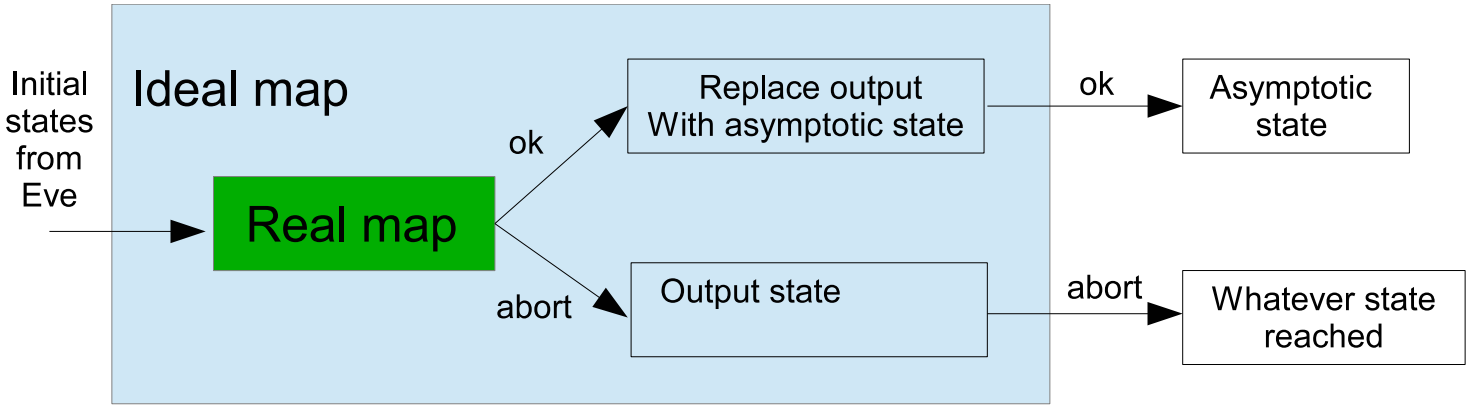

Figure: Illustration of the ideal map $\mathcal{F}$: Internally it runs the real map $\mathcal{E}$ and depending on whether the protocol succeeds it replaces the final state after hashing with the asymptotic state. This abstracts the distillation protocol as a process.

The EDP $\mathcal{E}$ is defined to be confidential if $\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon$, see [5].

Confidentiality of noiseless hashing

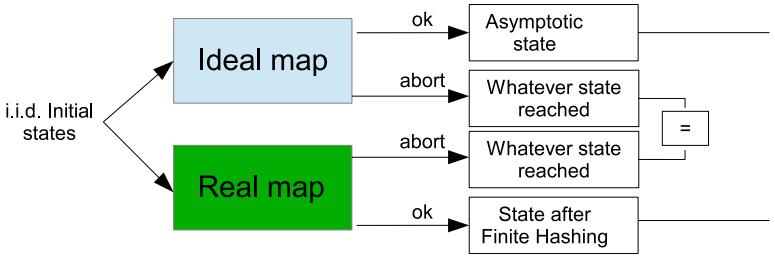

Figure: The figure illustrates the real map $\mathcal{E}$ and the ideal map $\mathcal{F}$ $\Rightarrow$ we only need to concern the ok-branch!

We compute $\|(\mathcal{E}-\mathcal{F})(\rho^{\otimes n+kn})\|_1 \leq \varepsilon_{\mathrm{H}}$ where $\varepsilon_{\mathrm{H}} \in O(\exp(-n^{3/5}))$ and we find via the post-selection technique [6] that

$$\|\mathcal{E}-\mathcal{F}\|_\diamond \leq 4 g_{n+kn,d} \sqrt{\max_{\sigma_{AB}} \left\| (\mathcal{E}^h - \mathcal{F}^h)\left(\sigma_{AB}^{\otimes n+kn}\right)\right\|_1} \leq 4 g_{n+kn,d}\sqrt{\varepsilon_{\mathrm{H}}}$$

where $g_{n+kn,d} = \binom{n+kn+d^2-1}{n} \leq (n+kn+1)^{d^2-1}$.

Confidentiality of noisy hashing

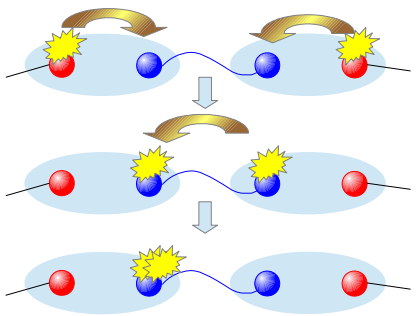

Figure: The figure shows the basic principle how we move the noise of the resource states to one side [7].
$\Rightarrow$ modify parameter estimation.

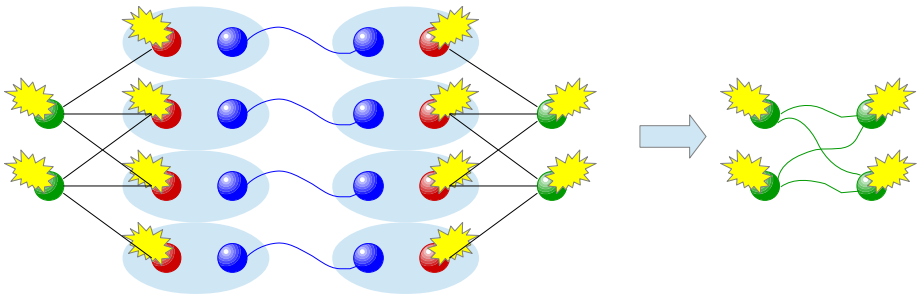

Figure: The protocol considering LDN $\mathcal{N}^\alpha$ on the output qubits corresponds to a noiseless protocol followed by LDN (which is CPTP).

So we conclude

$$\begin{aligned}\|\mathcal{E}^\alpha - \mathcal{F}^\alpha\|_\diamond &= \|\mathcal{N}^\alpha \circ (\mathcal{E}^{\alpha-\mathrm{in}} - \mathcal{F}^{\alpha-\mathrm{in}})\|_\diamond \\ &\leq \|\mathcal{E}^{\alpha-\mathrm{in}} - \mathcal{F}^{\alpha-\mathrm{in}}\|_\diamond = \|\mathcal{E} - \mathcal{F}\|_\diamond. \qquad (1)\end{aligned}$$

Quantum repeater via recurrence protocols

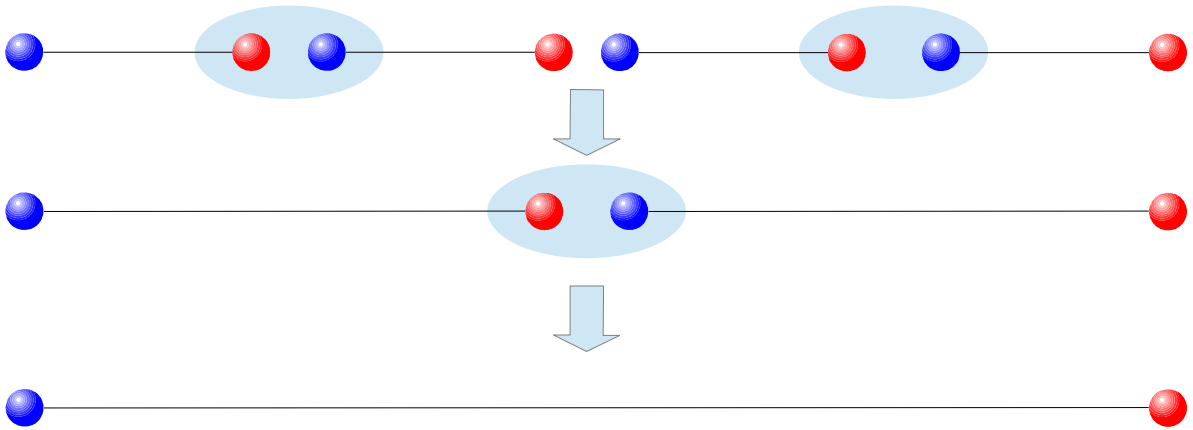

Figure: Illustration of the standard quantum repeater scheme [8, 9]: short-distance Bell-pairs get purified by recurrence-type distillation protocols and combined via entanglement swapping to establish long-distance Bell-pairs in a nested fashion.

Quantum repeater via hashing protocol

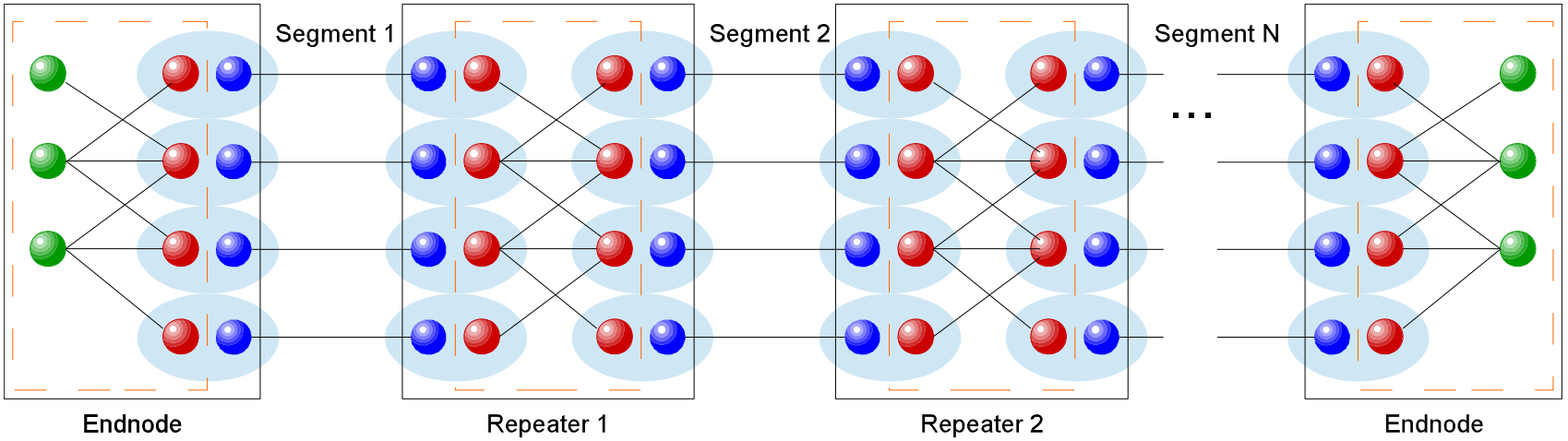

Figure: Quantum repeater based on measurement-based hashing [10]: We divide the channel into N segments, each comprising several Bell-pairs. The repeaters couple their parts of the Bell-pairs to the resource states (hashing protocol + entanglement swapping) simultaneously.

Quantum repeater via hashing protocol

The global fidelity relative to $m = n(1 - S(\rho) - 2\delta)$ systems in the $|\phi^+\rangle$ state for N segments satisfies

$$F \geq \left(1 - \alpha \exp(-\beta n \delta^2)\right)^N \approx 1 - N\alpha \exp(-\beta n \delta^2)$$

where α, β are constants depending on the initial pairs and δ is tunable parameter vanishing in the large n limit.
The overhead O of the protocol reads as

$$O = 2(1 - S(\rho) - 2\delta)^{-1}.$$

$\Rightarrow$ is independent of N and approaches a constant for the limit of large n! (which is in contrast to the standard repeater schemes)

Quantum repeater via hashing protocol

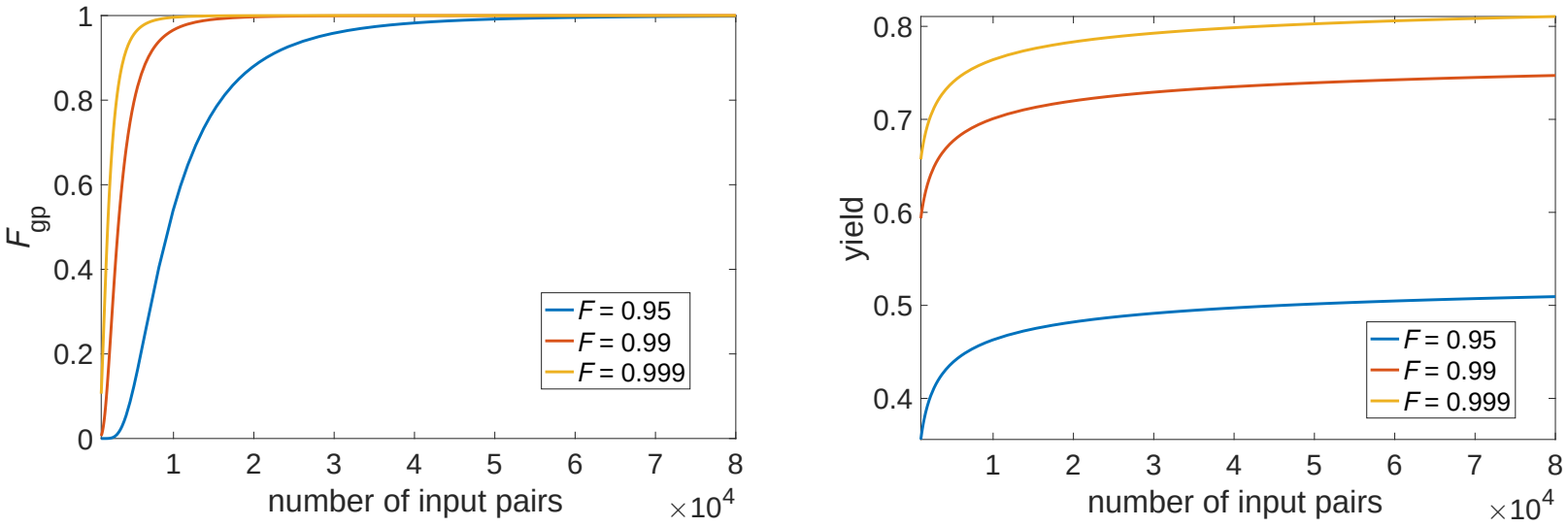

Figure: The figures show the results for $N = 100$ segments and 1% i.i.d. LDN acting on the resource states. Left: scaling of the global fidelity. Right: yield of protocol, i.e. the fraction of purified output pairs and noisy input pairs.

Quantum repeater via hashing protocol

We highlight the advantages of the quantum repeater via hashing as follows:

- *Deterministic* implementation
- *Constant* local overhead
- *Parallel* generation of several Bell-pairs

References I

[1] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. 77, 2818 (1996).

[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. 76, 722 (1996).

[3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 54, 3824 (1996).

[4] M. Zwerger, H. J. Briegel, and W. Dür, Phys. Rev. A 90, 012314 (2014).

[5] A. Pirker, V. Dunjko, W. Dür, and H. J. Briegel, arXiv:1610.01907 (2016)

References II

[6] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. 102, 020504 (2009)

[7] M. Zwerger, H. J. Briegel, and W. Dür, Phys. Rev. Lett. 110, 260503 (2013).

[8] W. Dür, H. J. Briegel, J. I. Cirac, P. Zoller, Phys. Rev. A 59, 169-181 (1999).

[9] H. J. Briegel, et. al., Phys. Rev. Lett. 81, 5932 (1998).

[10] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, W. Dür, arXiv:1705.02174 (2017).

Thank you!