A comparison of three entanglement distillation protocols in the presence of noise

Siem van Benthem S.VANBENTHEM@STUDENT.TUDELFT.NL
Rik Ledoux R.M.LEDOUX@STUDENT.TUDELFT.NL
Benjamin Oudejans B.C.OUDEJANS@STUDENT.TUDELFT.NL
Delft Institute of Applied Mathematics, Delft University of Technology, the Netherlands

Abstract

This study compares the performance of three distillation protocols in the presence of noise in both quantum gates and network links in order to determine which has the best performance. Performance of distillation protocols is important, since entangled states with high fidelity are desired for many applications in quantum computing, such as quantum teleportation. The protocols in question are the BBPSSW protocol (Bennett et al., 1996), the DEJMPS protocol (Deutsch et al., 1996) and the distillation scheme by Chi et al. (2012), called the three-to-one protocol. The research questions were answered by means of simulations with the aid of a quantum network simulator. The results show that three-to-one protocol outperforms both the BBPSSW and DEJMPS protocols and that the DEJMPS protocol performs worst.

1. Introduction

In recent years, quantum technology has been developing quickly, allowing for more and more real-world applications of quantum networking. One important component of many quantum networking applications is entanglement distillation, which can increase the fidelity of entangled states between nodes in a network.

As is well known, quantum computers pose a threat to classical cryptography, but quantum technology also provides solutions in many ways, such as in the form of quantum key distribution. It allows for completely secure network protocols in which eavesdroppers have no way to read messages over the network, something that is not possible via classical communication over public channels. However, all of these applications require two parties to share an entangled state, and this entanglement is not trivial to accomplish. Since a single qubit is represented by a single elementary particle, e.g. a photon, it is much more susceptible for noise than a classical bit, which can be represented by an arbitrary amount of photons. On sending a qubit over a network, it will become entangled with the environment, and thus the fidelity of the entangled pair with respect to their original state decreases. As for many applications high fidelity entangled pairs are desirable, this loss of fidelity may be problematic.

At this point, entanglement distillation protocols may come to the rescue. These protocols are designed to, given two (or more) entangled input states of imperfect fidelity shared by two nodes, create one shared output state with increased fidelity, at the cost of destroying the other input pairs. In this report we will discuss several of these protocols: the DEJMPS protocol by Deutsch et al. (1996), the BBPSSW protocol by Bennett et al. (1996) and the three-to-one protocol by Chi et al. (2012). Each of these protocols has their strengths and weaknesses: The DEJMPS protocol can be easily iterated, however, each iteration yields only a small improvement regarding the fidelity. The conditions for iteration of the BBPSSW are more complicated, as it can only be applied to exact copies of states. It might however reach obtain a higher fidelity in less iterations. The three-to-one protocol also yields a high fidelity, but costs more entangled pairs to produce. We will discuss the characteristics each of these protocols in more detail in Section 3.2.

Before doing so, we will first state the aims of this research in Section 2. Then, after discussing our research model and the protocols in Section 3, we will state our results in Section 4 and discuss them in Section 5.

2. Research question

We will investigate which of the three aforementioned protocols has the best performance in a simulated quantum network, over a range of simulation parameters. The parameters that will be varied are the link

fidelity of the network link, and the gate fidelity of the sender and receiver nodes. In order to be able to do a reflection on the qualities of the three protocols under consideration, we will quantify their behaviour with regard to three properties.

First, by varying both the gate fidelity and link fidelity parameters, we determine which combinations yield a feasible setting, i.e. a setting in which for each individual protocol, the output state has higher fidelity than the input state, when the protocol is successful. Then, for each of the protocols and for some appropriate settings of the gate fidelity parameter, we will determine how the ratio $F_{\text{out}}/F_{\text{in}}$ depends on the input fidelity. Thirdly, for the same settings of the gate fidelity parameter we will gather statistics on the success probability p_{succ} of each protocol.

The results of these measurements will then be collected in a single criterion of judgement: *the relative improvement*, defined as

$$\frac{F_{\text{out}} - F_{\text{in}}}{n\, F_{\text{in}}} p_{\text{succ}}, \tag{1}$$

where n is the number of input EPR pairs required for the protocol. The relative improvement can be thought of as the expected improvement (given success) per EPR pair, multiplied with the success probability. We will use this to quantify the quality of each protocol.

3. Method

3.1. Model

Our aim is to answer the research questions in Section 1 by simulating the protocols in question using the quantum network simulation tool netqasm. We will use the network settings `gate-fidelity` and `fidelity` to vary the gate fidelity of the nodes and the fidelity of the links respectively.

By variation and interpolation we will determine for each value of the gate fidelity parameter on which input states the protocols are able to accomplish an increase in fidelity. For two values of the gate fidelity parameter we will plot the curve of the ratio $F_{\text{out}}/F_{\text{in}}$ of the output and input state fidelities as a function of the input state fidelity. We will do this for both perfect gates (parameter fixed at 1) and for noisy gates, where we let the value of the parameter be determined by the previous question. By repeated simulation we will then determine the approximate rate of success p_{succ} of the protocols for the same two values of the gate fidelity.

To conclude our investigations into the three distillation protocols, we will combine these results to find the relative improvement for each protocol, as given in Equation (1). This formula will be the major criterion in answering the main research question.

Before we continue to the presentation of our findings and results, we will briefly discuss some of the characteristics of each protocol in the remainder of this section.

3.2. Protocols

3.2.1. DEJMPS

The DEJMPS protocol described in Deutsch et al. (1996) is an iterative entanglement distillation protocol that allows one to create a pair of qubits of fidelity arbitrarily close to 1 with respect to the state $|\Phi_{00}\rangle$. The algorithm requires the sender and receiver to share two pairs of entangled qubits. One notable property of this protocol is that it is cryptographically safe: these pairs of qubits may be prepared by an eavesdropper in any state, including being entangled to other qubits that the eavesdropper has in their possession. Applying this protocol repeatedly reduces the entanglement of Alice and Bob's qubits to any outside system to an arbitrarily low level, so any eavesdropper would not be able to gain information on what Alice and Bob do to their qubits.

The algorithm works by applying the gate $R_x\left(\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}$ (in the z-basis) to each of Alice's qubits, and the inverse gate $R_x\left(-\frac{\pi}{2}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$ to each of Bob's. Then both Alice and Bob apply a CNOT gate to their qubits, using the first pair as controls and the second pair as the targets. Lastly they measure their second qubits, and if the measurement outcomes are the same, distillation is successful and the first pair is kept. Otherwise both pairs are discarded. In the case of success, we can apply the protocol again to iteratively get a better state.

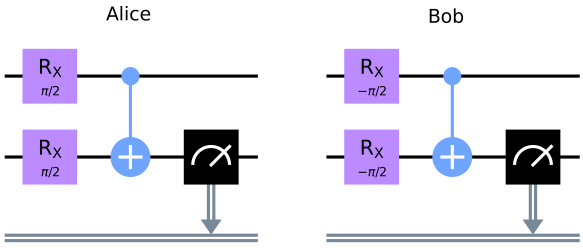

Figure 1: Alice and Bob's circuits for the DEJMPS protocol.

Assuming the qubit pairs are not entangled to any external state, we can write the state as diagonal in the Bell basis:

$$\rho_{\text{in}} = A\,|\Phi_{00}\rangle\langle\Phi_{00}| + B\,|\Phi_{11}\rangle\langle\Phi_{11}| + C\,|\Phi_{01}\rangle\langle\Phi_{01}| + D\,|\Phi_{10}\rangle\langle\Phi_{10}|$$

Then the outcome state will have new coefficients in the Bell basis:

$$\tilde{A} = \frac{A^2+B^2}{p_{\text{succ}}} \quad \tilde{B} = \frac{2CD}{p_{\text{succ}}}$$
$$\tilde{C} = \frac{C^2+D^2}{p_{\text{succ}}} \quad \tilde{D} = \frac{2AB}{p_{\text{succ}}}$$

where $p_{\text{succ}} = (A+B)^2 + (C+D)^2$ is the probability of success.

Note that $A = \langle\Phi_{00}|\rho_{\text{in}}|\Phi_{00}\rangle$ is the fidelity of the state. Hence the first of the above equations tells us how much the fidelity improves. If we use a Werner state

$$\rho_{\text{in}} = p\,|\Phi_{00}\rangle\langle\Phi_{00}| + \frac{1-p}{4}\mathbf{1}_4$$

as input, we can compute that the fidelity is $F_{\text{in}} = \frac{3p+1}{4}$. Then it follows after some computation that

$$p_{\text{succ}} = \frac{8F_{\text{in}}^2 - 4F_{\text{in}} + 5}{9}$$

After successful distillation, the outcome fidelity is

$$F_{\text{out}} = \tilde{A} = \frac{10F_{\text{in}}^2 - 2F_{\text{in}} + 1}{8F_{\text{in}}^2 - 4F_{\text{in}} + 5}$$

3.2.2. BBPSSW

The BBPSSW protocol by Bennett et al. (1996) is a protocol that is in the limit capable of creating an EPR pair with fidelity (with respect to any Bell state) arbitrarily close to 1, by iteratively applying some purifying steps.

The iterative part works as follows (Bennett et al., 1996): Under the assumption of having noiseless gates, each iteration requires two EPR pairs of identical fidelity $F_{\text{in}} > \frac{1}{2}$ (with respect to the state $|\Phi_{00}\rangle$, possibly after applying some rotation) as an input shared by both nodes. These can be for example two copies of the Werner state

$$\rho_{\text{in}} = p\,|\Phi_{00}\rangle\langle\Phi_{00}| + \frac{1-p}{4}\mathbf{1}_4,$$

with $p > \frac{1}{3}$. The iteration then outputs a single EPR pair of increased fidelity with a certain probability. During the iteration, the nodes perform a bilateral local CNOT operation with the first qubit as the control qubit, and the second one as the target. Then they both measure the spin of the second qubit in the z-basis and use classical communication to inform one another on the outcome. They keep the remaining qubit only if the measurement outcomes agree. It then has an increased fidelity of

$$F_{\text{out}} = \frac{F_{\text{in}}^2 + \frac{1}{9}(1-F_{\text{in}})^2}{F_{\text{in}}^2 + \frac{2}{3}F_{\text{in}}(1-F_{\text{in}}) + \frac{5}{9}(1-F_{\text{in}})^2}.$$

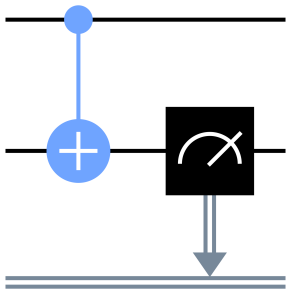

Figure 2: The circuit that both Alice and Bob execute to perform the BBPSSW protocol.

The probability of success is (Dür and Briegel, 2007):

$$p_{\text{succ}} = F_{\text{in}}^2 + 2F_{\text{in}}(1-F_{\text{in}})/3 + 5[(1-F_{\text{in}})/3]^2$$

(matching the denominator of the output fidelity), which can be simplified to $(8F_{\text{in}}^2 - 4F_{\text{in}} + 5)/9$, which is a parabola that has its minimum $(1/2)$ at $F_{\text{in}} = \frac{1}{4}$ and increases to 1 as $F_{\text{in}} \uparrow 1$. One can check that the values of the output fidelity resp. the probability of success of the DEJMPS and BBPSSW protocols exactly match.

A major drawback of this protocol is that the output state is no longer a Werner state, and the protocol requires the nodes to randomly apply a bilateral rotation in each iteration to overcome this problem. The stated expressions assume perfect gates. Now whenever the gate fidelity of either nodes is smaller than 1, this will assuredly deteriorate the efficiency and the upper limit of the protocol.

Another drawback is that to output a single purified EPR pair (over a single iteration), the model consumes in expectation $\frac{2}{p_{\text{succ}}}$ input EPR pairs. Iterating the pu-

rification N times thus requires[1] $\prod_{n=1}^{N} \frac{2}{p_{\text{succ},n}} > 2^N$ EPR pairs: an exponential growth in N.

3.2.3. THREE-TO-ONE

The protocol described by Chi et al. (2012) differs from the BBPSSW and DEJMPS protocol in that it uses three EPR pairs, rather than two. For this reason, this protocol will be referred to as the three-to-one protocol. The three-to-one protocol is one of the first distillation procedures for which the efficiency (success probability per entangled input pair), under noiseless conditions, exceeds the efficiency of the BBPSSW protocol by Bennett et al. (1996). Furthermore, the three-to-one protocol can be adopted to improve the efficiency of the Metwally protocol by Metwally (2002), which was the best existing two-to-one protocol in 2012.

The three-to-one protocols follows these instructions, which are for a one round distillation scheme. It starts with three Werner states ρ_{in} (same as before) with $F_{\text{in}} > \frac{1}{2}$ (with respect to the target state $|\Phi_{00}\rangle\langle\Phi_{00}|$). Notationwise, we write A_i and B_i for the qubits of the $i-$th Werner states, where qubit A_i is owned by Alice and B_i by Bob. After initialisation of the Werner states, four CNOT gates (first is the control qubit) are applied: $A_3 \rightarrow A_2, B_3 \rightarrow B_2, A_1 \rightarrow A_3, B_1 \rightarrow B_3$. Here, the first two CNOT gates are applied first (at the same time), which are then followed by the other two. Subsequently, a Bell measurement is performed on the two-qubit states corresponding to qubits A_1A_2 and B_1B_2. If the measurement outcomes are identical then the distillation procedure was successful and we have obtained a Werner state with higher fidelity, otherwise a failure is declared and the state of qubits A_3B_3 is discarded. A convenient visual representation of this protocol can be found in Figure **??**.

The performance of the three-to-one algorithm has already been assessed by Chi et al. (2012), and can be characterised neatly by formulas. The output fidelity F_{out} (for input fidelity F_{in}), is given by the formula

$$F_{\text{out}} = \frac{2 - 7F_{\text{in}} + 14F_{\text{in}}^2}{7 - 14F_{\text{in}} + 16F_{\text{in}}^2},$$

which is only valid for $F_{\text{in}} > \frac{1}{2}$ and satisfies $F_{\text{out}} > F_{\text{in}}$. The success probability is given by

$$p_{\text{succ}} = \frac{(1 + 2F_{\text{in}})(7 - 14F_{\text{in}} + 16F_{\text{in}}^2)}{27}.$$

1. Note that $p_{\text{succ},n}$ monotonically increases to 1 as the input fidelity of the n-th iteration increases to 1 (so as $n \rightarrow \infty$).

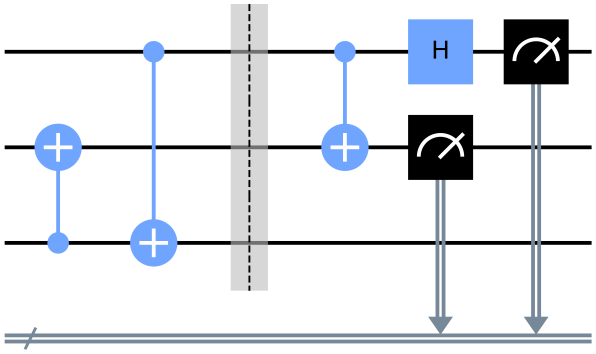

Figure 3: The circuit that Alice and Bob both execute on their qubits in the three-to-one distillation protocol. The circuit behind the dotted line performs a Bell measurement.

The three-to-one distillation scheme can also be iterated to obtain an output fidelity arbitrarily close to 1, given that $F_{\text{in}} > \frac{1}{2}$. For this iterative procedure, the output states are used for the next round of the protocol, hence for an N-round scheme, one would need at least 3^N initial Werner states (exactly 3^N if each round is successful). The formulas for the output fidelity and success probability are of course still valid for the iterative scheme, given that the input fidelity is replaced by the output fidelity of the previous round.

4. Numerical results

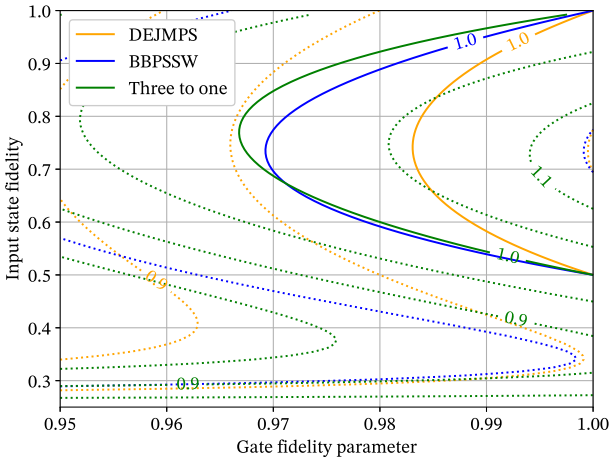

Figure 4: Contour plot of the ratio of the output fidelity over the input fidelity as function of the link and gate fidelity for the three protocols.

The first question we investigated was how well the different protocols perform as a function of the input state fidelity and the fidelity of the gates. Our question in this regard was, given nodes that can apply gates with a certain fidelity, what is the minimal amount of fidelity on the input states for the protocol to be able to improve the fidelity, i.e. to produce an output state of higher fidelity. We modelled this by collecting statistics on the output state fidelity for varied values of input state fidelity and gate fidelity, ranging the input state fidelity from 0.25 to 1 and the gate fidelity parameter from 0.95 to 1.

We present our results in the form of a contour plot in Figure 4, showing the isarithms of the ratio $F_{\text{out}}/F_{\text{in}}$. The solid curves represent the fraction 1.0 and indicate the equilibria: for each protocol, if the combination of input state and gate fidelity lies to the right of the 1.0-isarithm, the output state fidelity will be higher, whereas points to the left of it produce an output state of lower fidelity.

We observe that the areas on which we can expect improvement for each of the protocols forms a convex set in the top right corner op the plot. The plot illustrates that the capability of the DEJPMS protocol depends more heavily on the gate fidelity than the other two protocols. For the BBPSSW and the three-to-one protocol, the 1.0-isarithms roughly agree. The three-to-one protocol still seems to perform slightly better with respect to lower values of gate fidelity. Also, isarithms of the three-to-one protocol lie closer to each other, from which we conclude that the overall performance of this algorithm seems best with respect to this criterion. [2]

To ensure all protocols may perform relatively well, for the rest of our investigation we considered two cases: perfect (noiseless) gates and gates with a fidelity parameter of 0.99. For the latter value, all three protocols have quite a big range of input fidelities for which they perform well.

In Figures 5 and 6 we plotted the result for our second question, namely how the output fidelity improves (or worsens) as a function of the fidelity of the input states. These figures basically form a cross section of the contour plots at gate fidelity parameters 1.0 and 0.99. It is immediately seen that DEJMPS and BBPSSW perform the same when the gates are considered noiseless, and

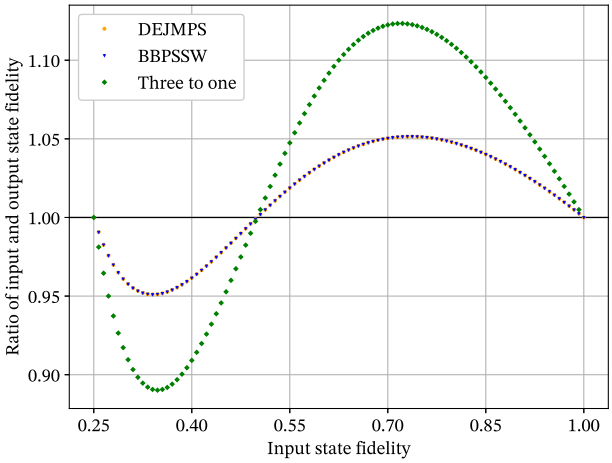

Figure 5: The ratio of the output fidelity over the input fidelity as function of the link and gate fidelity for the three protocols, with the gate fidelity parameter fixed at 1.0. The values of the DEJMPS protocol can hardly be distinguished in this plot, since they are overlapped by the values of the BBPSSW protocol.

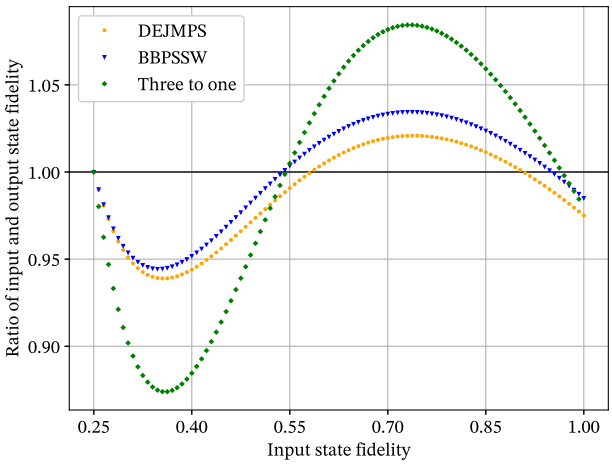

Figure 6: The ratio of the output fidelity over the input fidelity as function of the link and gate fidelity for the three protocols, with the gate fidelity parameter fixed at 0.99.

the three-to-one protocol performs much better; the improvement seems to be roughly 2.5 times as good.

If we move from Figure 5 to Figure 6 (i.e. if we change the gate fidelity parameter from 1.0 to 0.99), we see that the DEJMPS protocol is most susceptible for gate noise (which agrees to our findings from Figure 4). This is not completely surprising, as DEJMPS uses 6 gates in the protocol, whereas BBPSSW uses only 2. It should be noted that the three-to-one protocol uses 8 gates, however, this protocol uses three EPR pairs rather than two.

2. For completeness we included more detailed plots for the individual protocols in Figures 11, 12 and 13 in the Appendix to this report. There we observe that the isarithms of the three-to-one protocol are much denser than those of the other protocols.

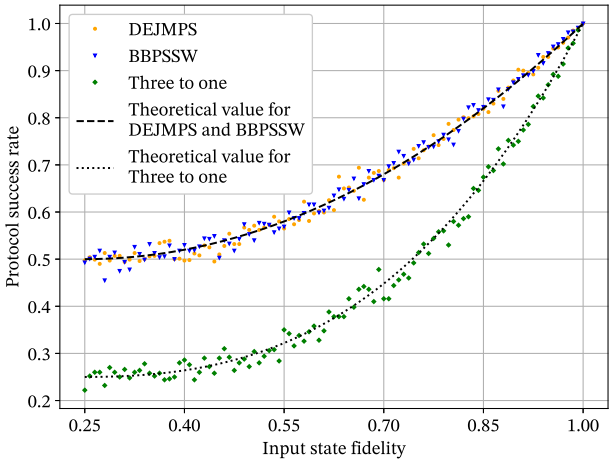

Figure 7: The rate of success of the three protocols over 1,000 attempts (500 for the three to one protocol), as function of the input state fidelity, with the gate fidelity parameter fixed at 1.0. The measured success rates concur with the theoretical values as described in Section 3.2.

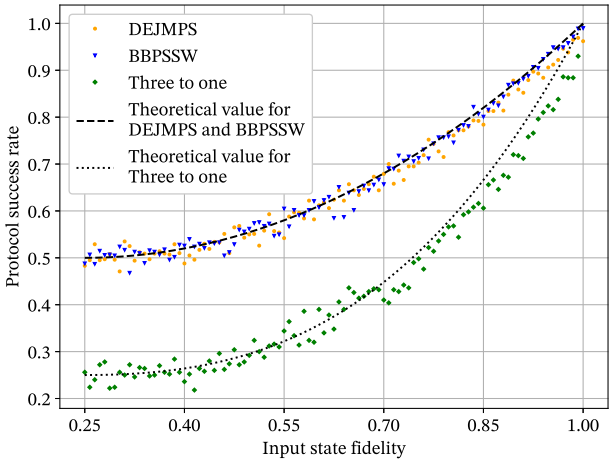

Figure 8: The rate of success of the three protocols over 1,000 attempts (500 for the three to one protocol), as function of the input state fidelity, with the gate fidelity parameter fixed at 0.99. Compared to the theoretical values computed for noiseless gates, the success rate at gate fidelity 0.99 has slightly dropped, which is best seen for the Three to one protocol and DEJMPS protocol.

Whereas the three-to-one protocol outperforms the DEJMPS and the BBPSSW protocols with respect to the ability to increase the fidelity, this improvement only happens on success. In Figures 7 and 8 we plotted the measured rate of success of the three protocols at gate fidelity of 1.0 and 0.99 respectively. The DEJMPS and BBPSSW protocols admit similar probabilities of success, but the success probability of the three-to-one protocol seems much lower whenever the input state fidelity is less than 1.

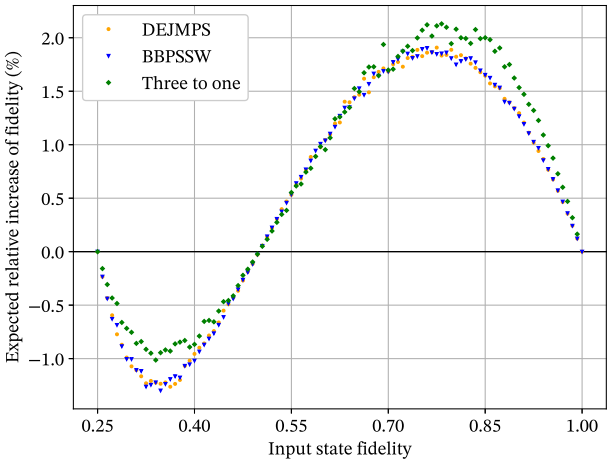

Figure 9: The expected relative improvement per consumed EPR pair for the three protocols as a function of the input fidelity, based on the experimental data, with the gate fidelity parameter fixed at 1.0.

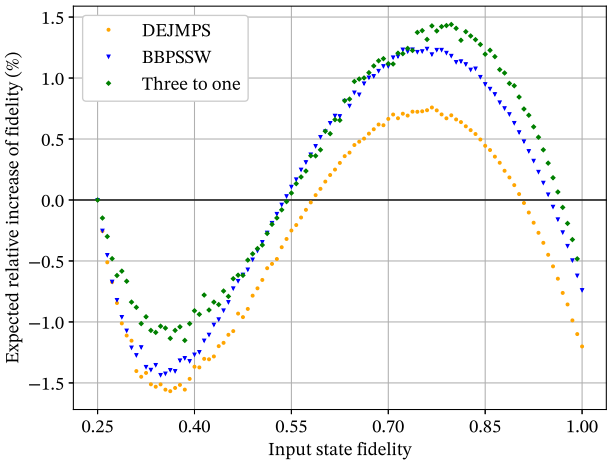

Figure 10: The expected relative improvement per consumed EPR pair for the three protocols as a function of the input fidelity, based on the experimental data, with the gate fidelity parameter fixed at 0.99.

In Figures 9 and 10 we plotted the expected relative improvement of the output fidelity over the input state per input EPR pair. In the case that both nodes can apply noiseless gates (Figure 9), if the input state fidelity is between 0.5 and roughly 0.6, there is hardly any difference regarding the performance of the three protocols. If the input state fidelity is higher, the three-to-one protocol slightly outperforms the other protocols, by at most 0.5 percentage point.

In the case of gates with fidelity 0.99 (Figure 10), the performance of the DEJMPS protocol rapidly drops, with the three-to-one protocol still slightly outperforming the BBPSSW protocol whenever the input state fidelity is larger than approximately 0.7.

5. Discussion

The overall conclusion from the numerical results is that in our simulated settings the three-to-one protocol outperforms the DEJMPS and BBPSSW protocols. In the case the nodes are not able to apply gates noiselessly, the DEJMPS protocol has the worst performance.

We must however remark that in our simulations, either one of the protocols was only performed once. One could repeat the protocols to achieve better results. The DEJMPS protocol only requires one extra EPR pair for each iteration, in the same state as the other input states. The other protocols need two (for the BBPSSW protocol), respectively three (for the three-to-one protocol) identical input states. One would thus require at least four, respectively nine EPR pairs to apply the protocol repetitively. The BBPSSW protocol also requires the application some random bilateral gates before the protocol can be iterated. In the case of noisy gates, the implementation of the random gates reduces the performance. More complicated simulations need to be performed to investigate the effect of iterating the protocols.

References

Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A., & Wootters, W. K. (1996). Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, *76*, 722–725. https://doi.org/10.1103/PhysRevLett.76.722

Chi, D., Kim, T., & Lee, S. (2012). Efficient three-to-one entanglement purification protocol. *Physics Letters, Section A: General, Atomic and Solid State Physics*, *376*(3), 143–146. https://doi.org/10.1016/j.physleta.2011.11.006

Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., & Sanpera, A. (1996). Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, *77*, 2818–2821. https://doi.org/10.1103/PhysRevLett.77.2818

Dür, W., & Briegel, H. J. (2007). Entanglement purification and quantum error correction. *Reports on Progress in Physics*, *70*(8), 1381–1424. https://doi.org/10.1088/0034-4885/70/8/r03

Metwally, N. (2002). More efficient entanglement purification. *Phys. Rev. A*, *66*, 054302. https://doi.org/10.1103/PhysRevA.66.054302

Appendix. Additional plots

In this appendix we include some plots that could be of interest for the reader, but that we kept out of the body of the text to preserve clarity.

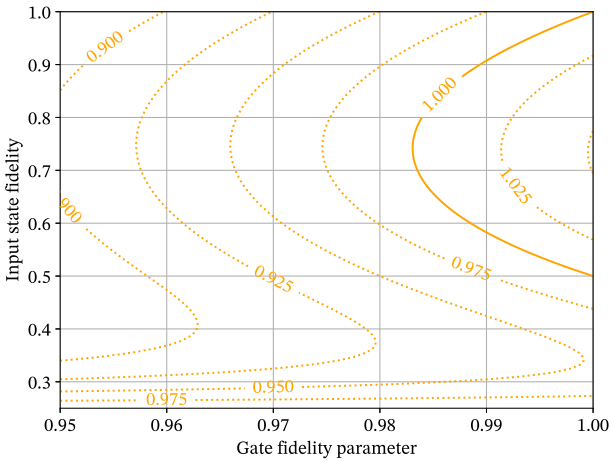

Figure 11: Contour plot of the ratio of the output fidelity over the input fidelity as function of the link and gate fidelity for the DEJMPS protocol.

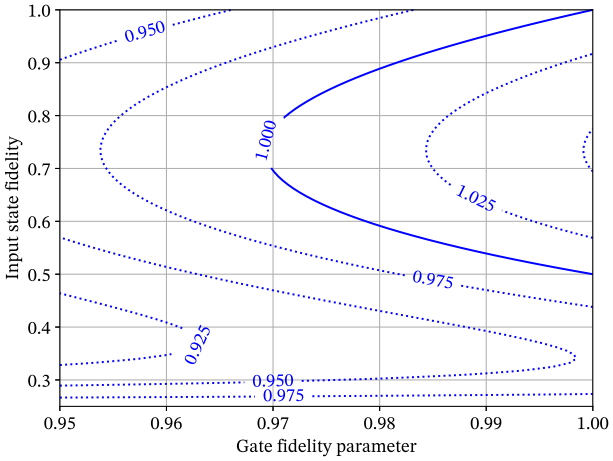

Figure 12: Contour plot of the ratio of the output fidelity over the input fidelity as function of the link and gate fidelity for the BBPSSW protocol.

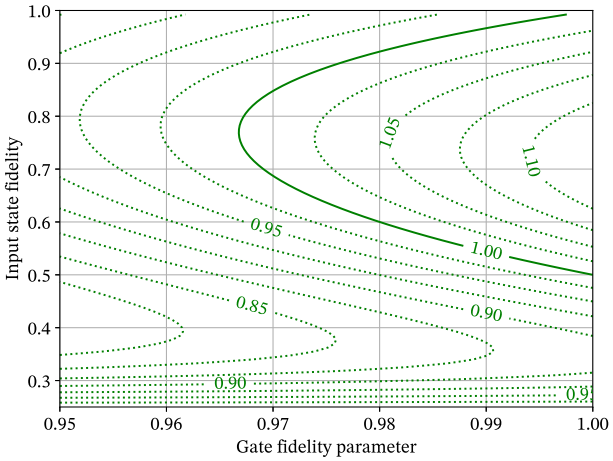

Figure 13: Contour plot of the ratio of the output fidelity over the input fidelity as function of the link and gate fidelity for the three-to-one protocol.