Comparing one- and two-way repeater architectures Supplementary Materials

Prateek Mantri, Kenneth Goodenough, and Don Towsley

Manning College of Information and Computer Sciences
University of Massachusetts Amherst, USA

Contents

1 Summary

1.1 Description of protocols

In this document we consider three multiplexed two-way (MTP) protocols,

1. **SKR rule based protocol:** Here the decision to distill is based on Secret Key Rate give by the following equation

$$f_{secret}(F_i^{\uparrow}) \cdot \mathbb{E}(Y_i^{\uparrow}) \underset{\mathcal{D}_i=0}{\overset{\mathcal{D}_i=1}{\gtrless}} f_{secret}(F_i) \cdot \mathbb{E}(Y_i), \forall i \in \{0, \cdots, n-1\} \tag{1}$$

where F_i is the fidelity of the state before distillation at level i, $Y_i^{\uparrow}$ denote the number of bell pairs on a segment at level i after one round of distillation, $F_i^{\uparrow}$ is the fidelity of the state after distillation at level i, and $f_{secret}(F)$ denote the secret-key fraction for a Bell pair with fidelity F, with the rest of variables bearing the same meaning and definition as in the main manuscript. The expected number of bell pairs at any level are computed as -

$$\mathbb{E}(Y_i) = \prod_{j=0}^{i}(1-r_j)^{\frac{N}{2^j}} \cdot \sum_{k=R_i}^{M_i} k \cdot p'_{i,k}, \forall i \in \{0, \cdots, n-1\} \tag{2}$$

$$\mathbb{E}(Y_i^{\uparrow}) = \prod_{j=0}^{i}(1-r_j)^{\frac{N}{2^j}} \cdot \sum_{k=R_i}^{\lfloor M_i/2 \rfloor} k \cdot q'_{i,k}, \forall i \in \{0, \cdots, n-1\} \tag{3}$$

2. **Always distill at elementary link level:** In this protocol, we fix $\mathcal{D}_0 = 1$, and the decision to distill at all levels except the elementary link level is based on the SKR rule outlined above.

3. **Always distill at all levels:** In this protocol, we fix $\mathcal{D}_i = 1 \quad \forall i \in 0, 1, \cdots, n-1$.

Besides these protocols we have also looked into a protocol based on fidelity threshold, however for brevity it has not been included in this document.

1.2 Description of parameter regimes

We consider four cases -

1. Low gate errors ($\epsilon_G = 10^{-4}$) and perfect coupling ($\eta_c = 1.0$)
2. Low gate errors ($\epsilon_G = 10^{-4}$) and imperfect coupling ($\eta_c = 0.9$)
3. Moderate gate errors ($\epsilon_G = 10^{-3}$) and perfect coupling ($\eta_c = 1.0$)
4. Moderate gate errors ($\epsilon_G = 10^{-3}$) and imperfect coupling ($\eta_c = 0.9$)

Additionally, for the SKR rule, we have included the performance plots for the different coupling and higher gate errors that have not been covered in the main text.

2 Always distill at elementary link protocol

2.1 Performance evaluation using secret-key rates

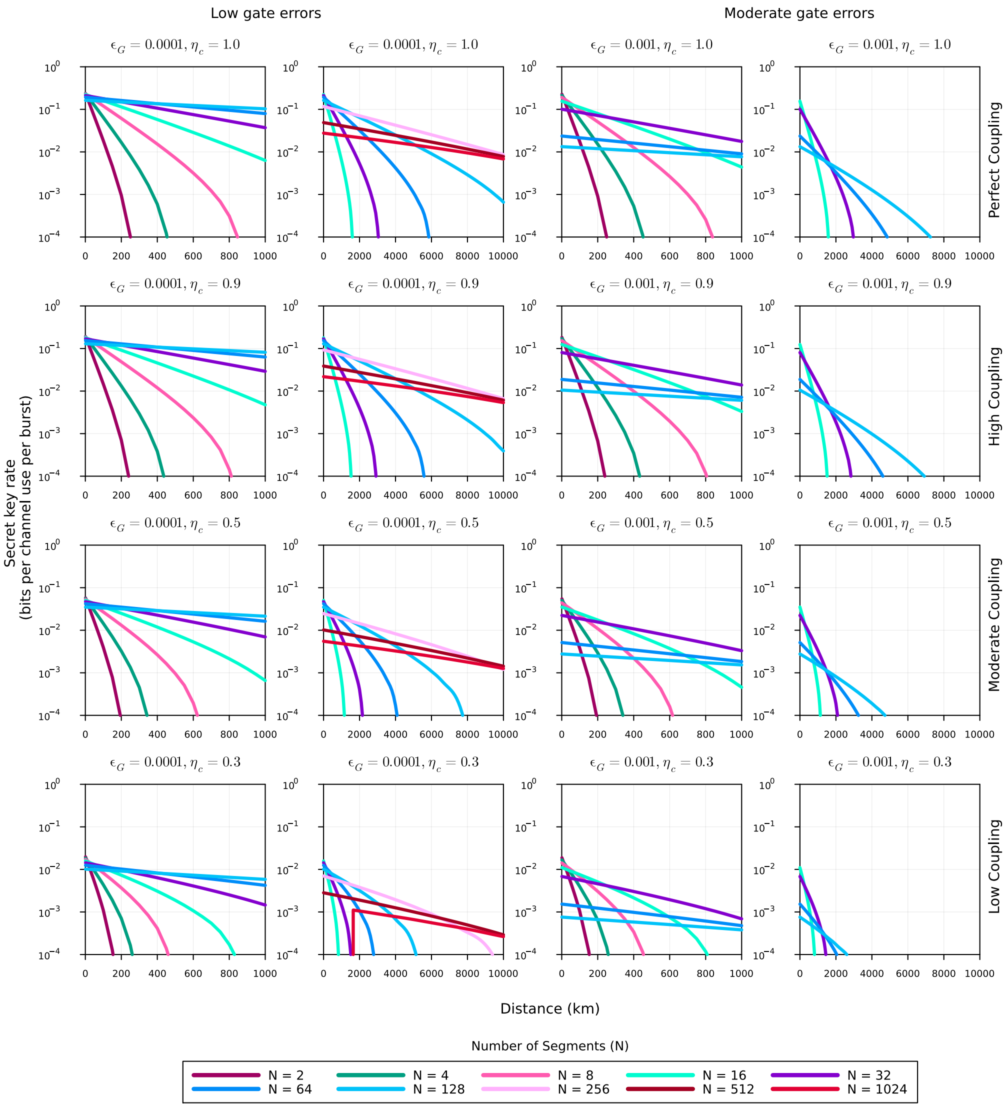

Figure 1: Performance of two-way multiplexed protocol with distance using secret key rate as the metric. The number of segments are shown in different colors and denoted by N. The left hand side plots consider a low gate error scenario with a gate error rate (ϵ_G) of 10^{-4} or 0.01%, and the right hand side plots shows the performance with moderate gate errors ($\epsilon_G = 10^{-3}$ or 0.1%). The different rows show the performance in different coupling regimes, starting with a perfect coupling ($\eta_c = 1$), with the coupling coefficient reducing with each successive row down ($\eta_c \in \{1, 0.9, 0.5, 0.3\}$). The odd columns (one and three) show the performance in the distance regimes of 1000 km and the even columns (two and fourth) show the performance in the 10000 km regime. In this setup we have used the protocol based on Secret Key Rate to inform the distillation decision making with a maximum of one round of distillation allowed at any level of nesting. However, one key difference between this protocol and the SKR based protocol is that a distillation operation always occur at the elementary link. Also, similar to all the MTP schemes considered, no distillation is performed at the end level.

2.2 Performance comparison using secret-key rates with QPC

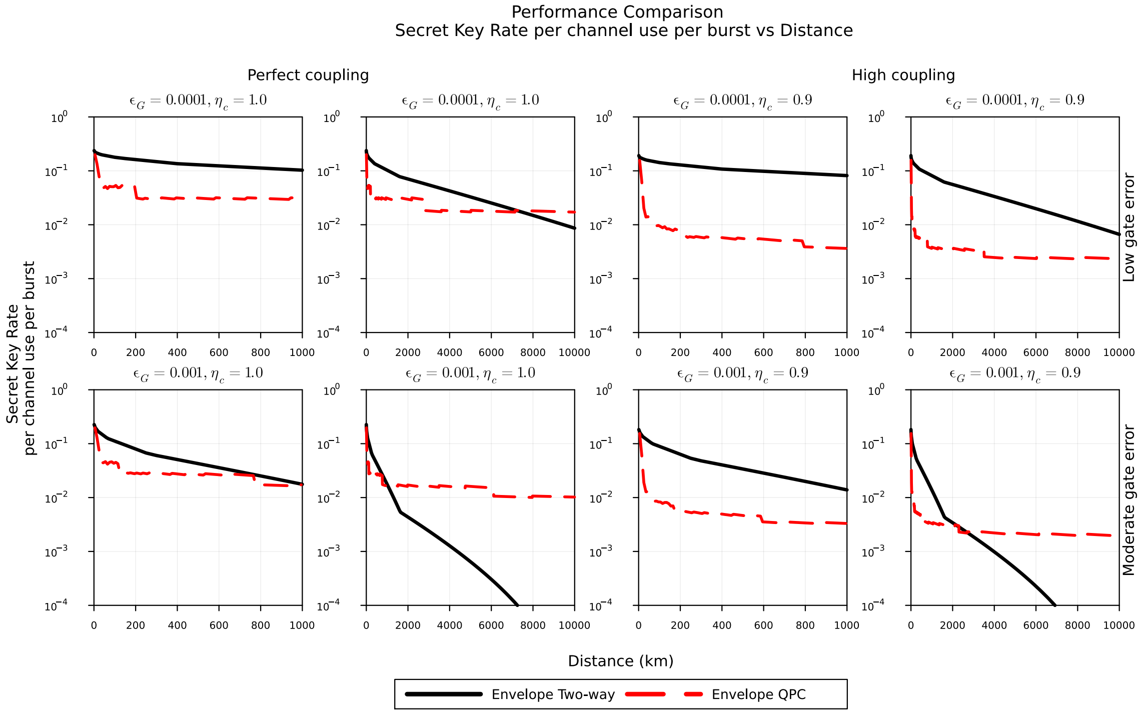

Figure 2: Performance comparison between one-way and two-way schemes using the secret-key rate as the metric. The red dashed line shows the performance by the optimal Quantum Parity Codes (QPC), and the black solid line is the envelope for the secret key rates for multiplexed two-way scheme (MTP) where a single distillation operation is compulsorily performed for the elementary link level. For each distance, a specific (n, m) QPC is chosen optimizing for total number of qubits required with the search parameters constrained to $n \leq 70, m \leq 20$. For this flavor of the MTP, a maximum of 1024 multiplexed channels have been considered. The MTP scheme delivers better secret key rates per channel use per burst in all parameter regimes except for very long distances in the case of moderate gate errors - i.e. distances $\gtrapprox$ 1000 km for perfect coupling regime, and $\gtrapprox$ 2200 km for high coupling regime.

2.3 Economy of architectures - comparison of resource costs

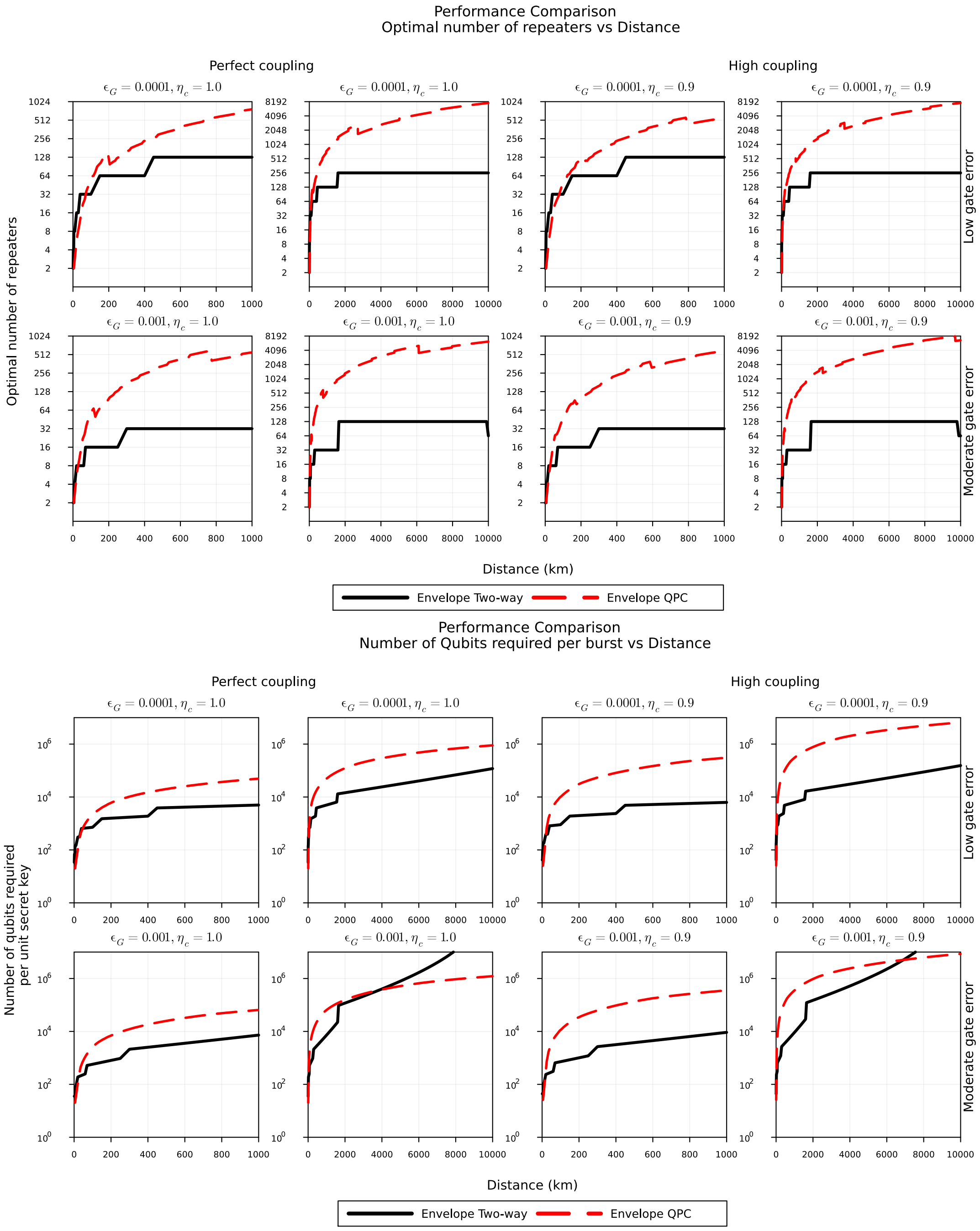

Figure 3: Number of (a) repeaters, and (b) qubits required per burst for each unit secret key delivered for optimal performance for one- and two-way repeater architectures. The red dashed line shows the number of repeaters required for the optimal Quantum Parity Code (QPC), and the black solid line is the envelope for the highest deliverable secret key rate for multiplexed two-way scheme (MTP) for any distance. To note, we do not consider the ancilla qubits required for state preparation, or teleportation based error correction for QPC, and the estimation presented here is a lower bound. For all parameter regimes considered, the MTP requires significantly less number of repeaters, and number of qubits than the QPC.

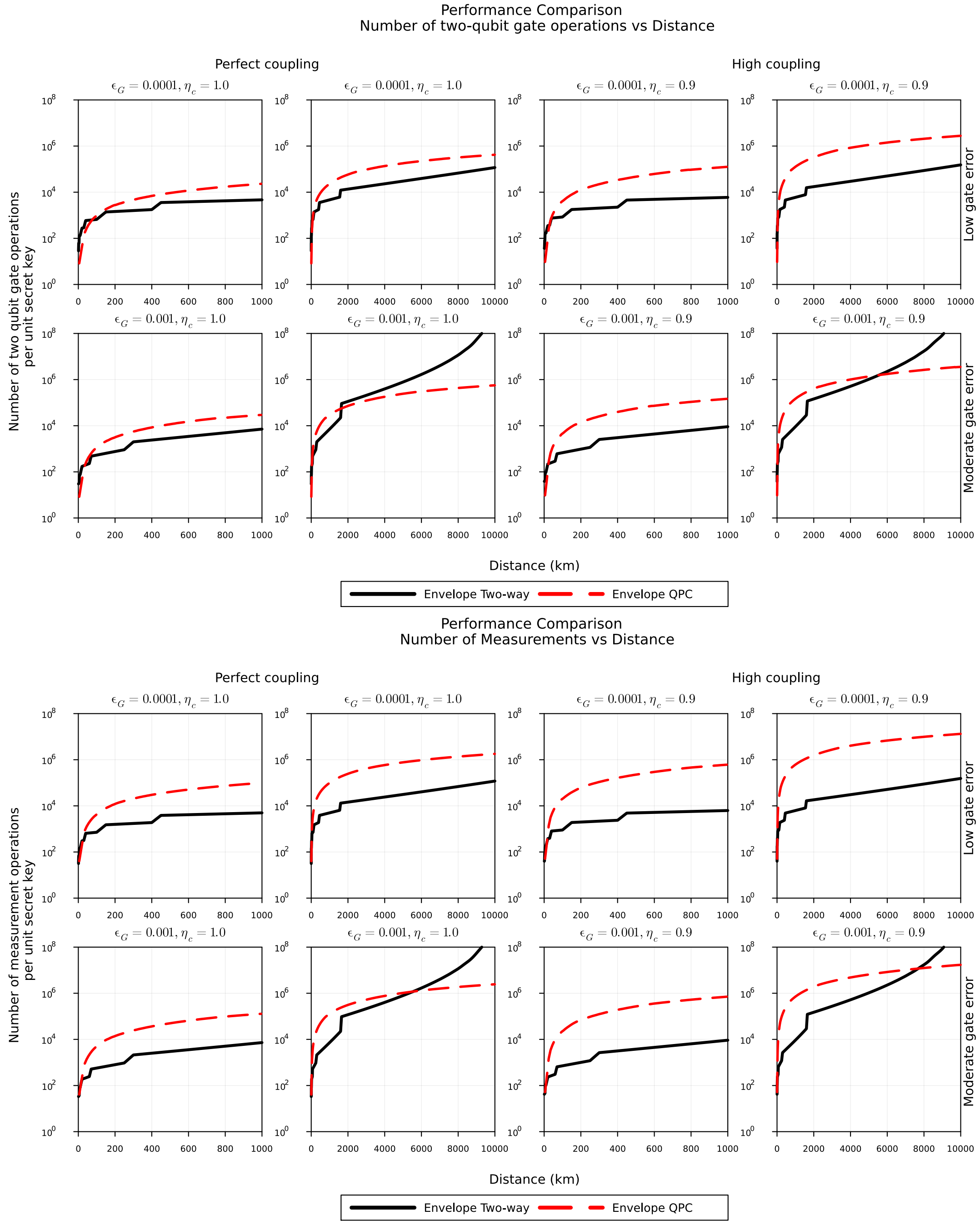

Figure 4: Number of (a) two-qubit gates and (b) measurement operations required per burst for each unit secret key delivered for one- and two-way repeater architectures. The red dashed line shows the number of repeaters required for the optimal Quantum Parity Code (QPC), and the black solid line is the envelope for the highest deliverable secret key rate for 'always distill at elementary link protocol' of the multiplexed two-way scheme (MTP) for any distance. To note, for QPCs, we have not considered gate operations required for state preparation or gate operations on ancilla qubits, and the estimation presented here is a lower bound. For almost all parameter regimes considered, the optimal QPC based protocol requires higher number of two-qubit gates and measurement operations than the MTP.

3 Always distill at all levels

3.1 Performance evaluation using secret-key rates

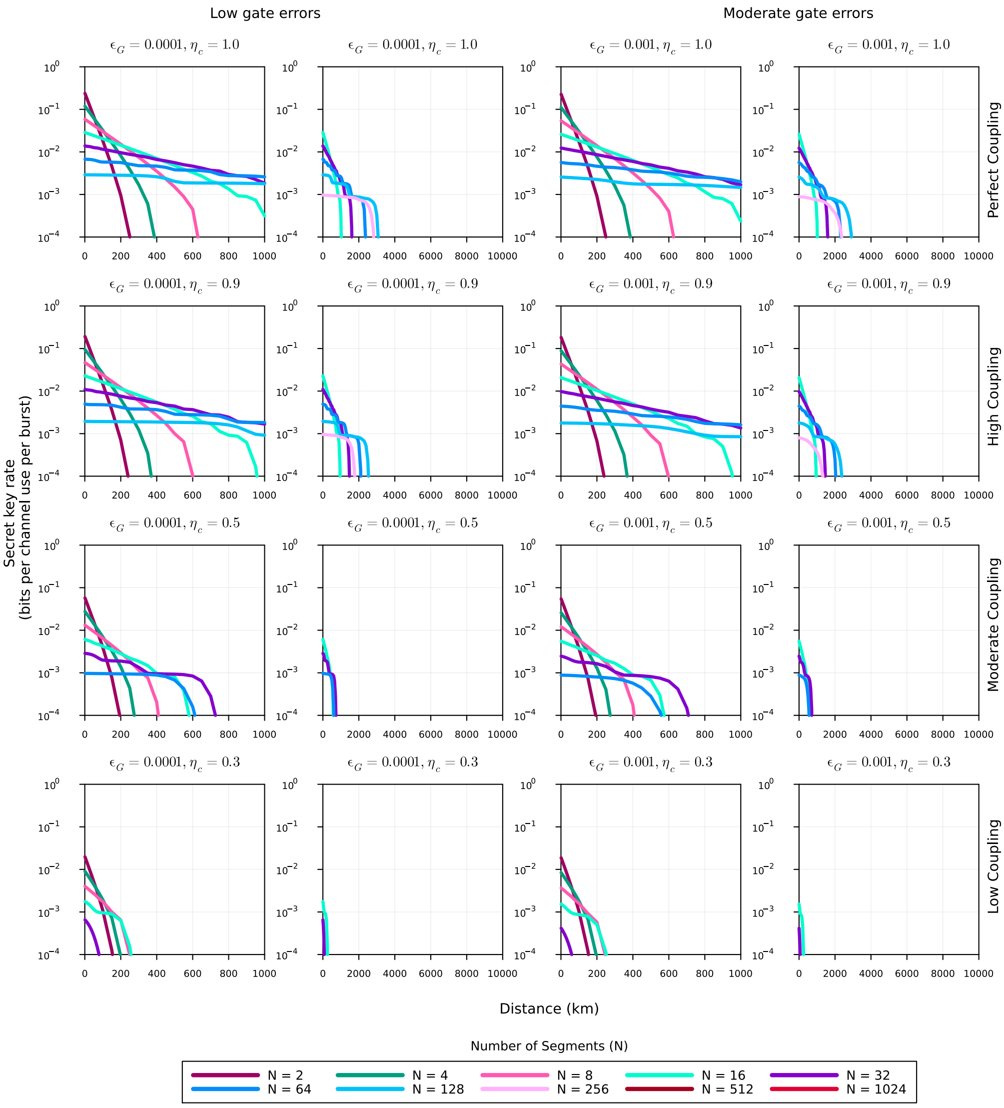

Figure 5: Performance of two-way multiplexed protocol with distance using secret key rate as the metric. The number of segments are shown in different colors and denoted by N. The left hand side plots consider a low gate error scenario with a gate error rate (ϵ_G) of 10^{-4} or 0.01%, and the right hand side plots shows the performance with moderate gate errors ($\epsilon_G = 10^{-3}$ or 0.1%). The different rows show the performance in different coupling regimes, starting with a perfect coupling ($\eta_c = 1$), with the coupling coefficient reducing with each successive row down ($\eta_c \in \{1, 0.9, 0.5, 0.3\}$). The odd columns (one and three) show the performance in the distance regimes of 1000 km and the even columns (two and fourth) show the performance in the 10000 km regime. In this setup we have used the protocol based on a static decision making with exactly one round of distillation performed at any level of nesting. Also, similar to all the MTP schemes considered, no distillation is performed at the end level.

3.2 Performance comparison using secret-key rates with QPC

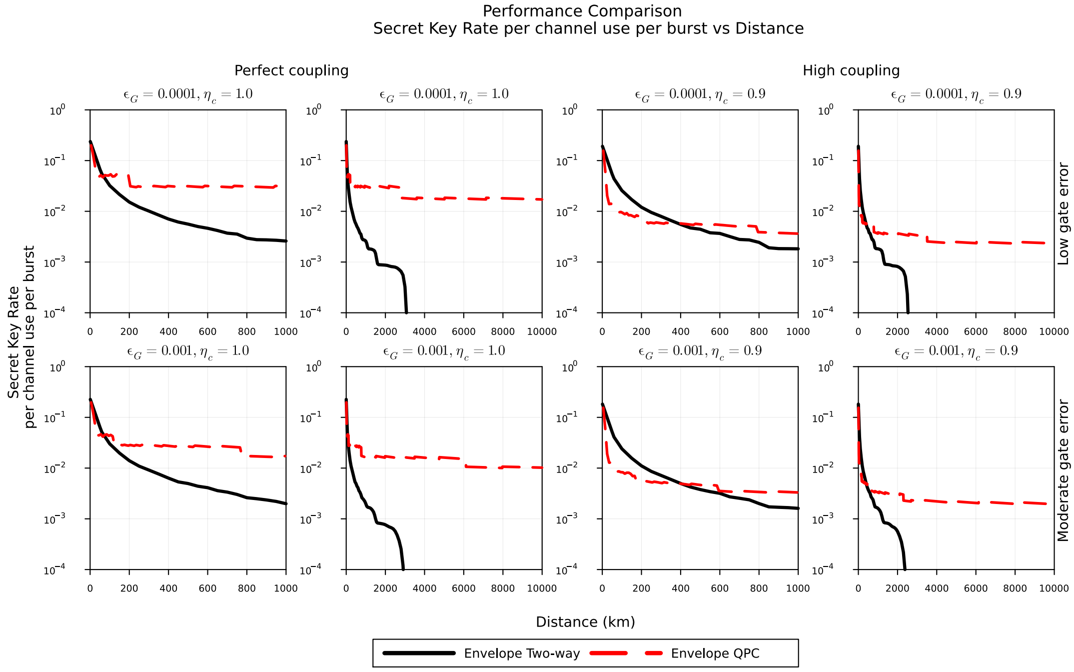

Figure 6: Performance comparison between one-way and two-way schemes using the secret-key rate as the metric. The red dashed line shows the performance by the optimal Quantum Parity Codes (QPC), and the black solid line is the envelope for the secret key rates for multiplexed two-way scheme (MTP) where a single distillation operation is compulsorily performed for the elementary link level. For each distance, a specific (n, m) QPC is chosen optimizing for total number of qubits required with the search parameters constrained to $n \leq 70, m \leq 20$. For this flavor of the MTP, a maximum of 1024 multiplexed channels have been considered.

3.3 Economy of architectures - comparison of resource costs

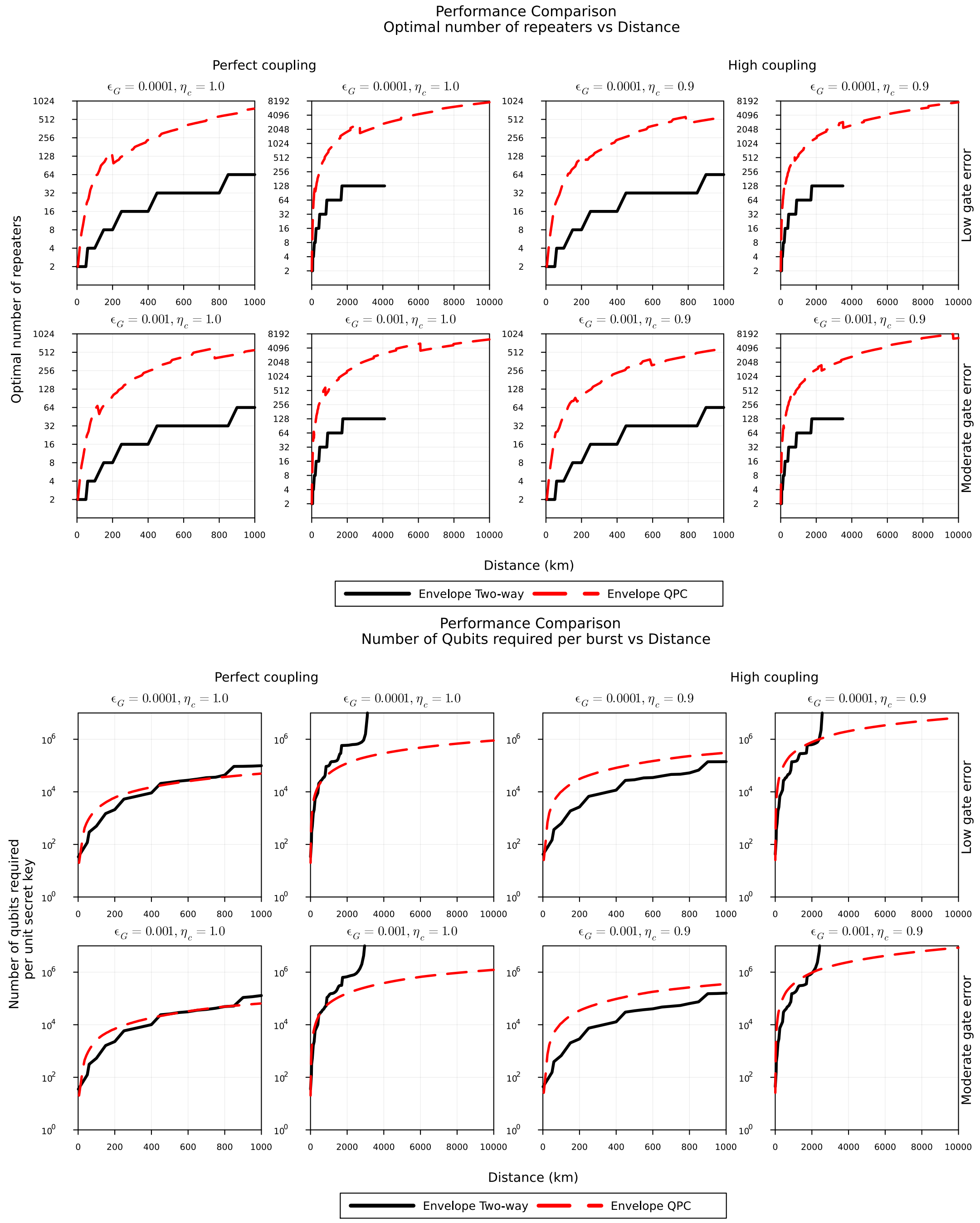

Figure 7: Number of (a) repeaters, and (b) qubits required per burst for each unit secret key delivered for optimal performance for one- and two-way repeater architectures. The red dashed line shows the number of repeaters required for the optimal Quantum Parity Code (QPC), and the black solid line is the envelope for the highest deliverable secret key rate for multiplexed two-way scheme (MTP) for any distance. To note, we do not consider the ancilla qubits required for state preparation, or teleportation based error correction for QPC, and the estimation presented here is a lower bound.

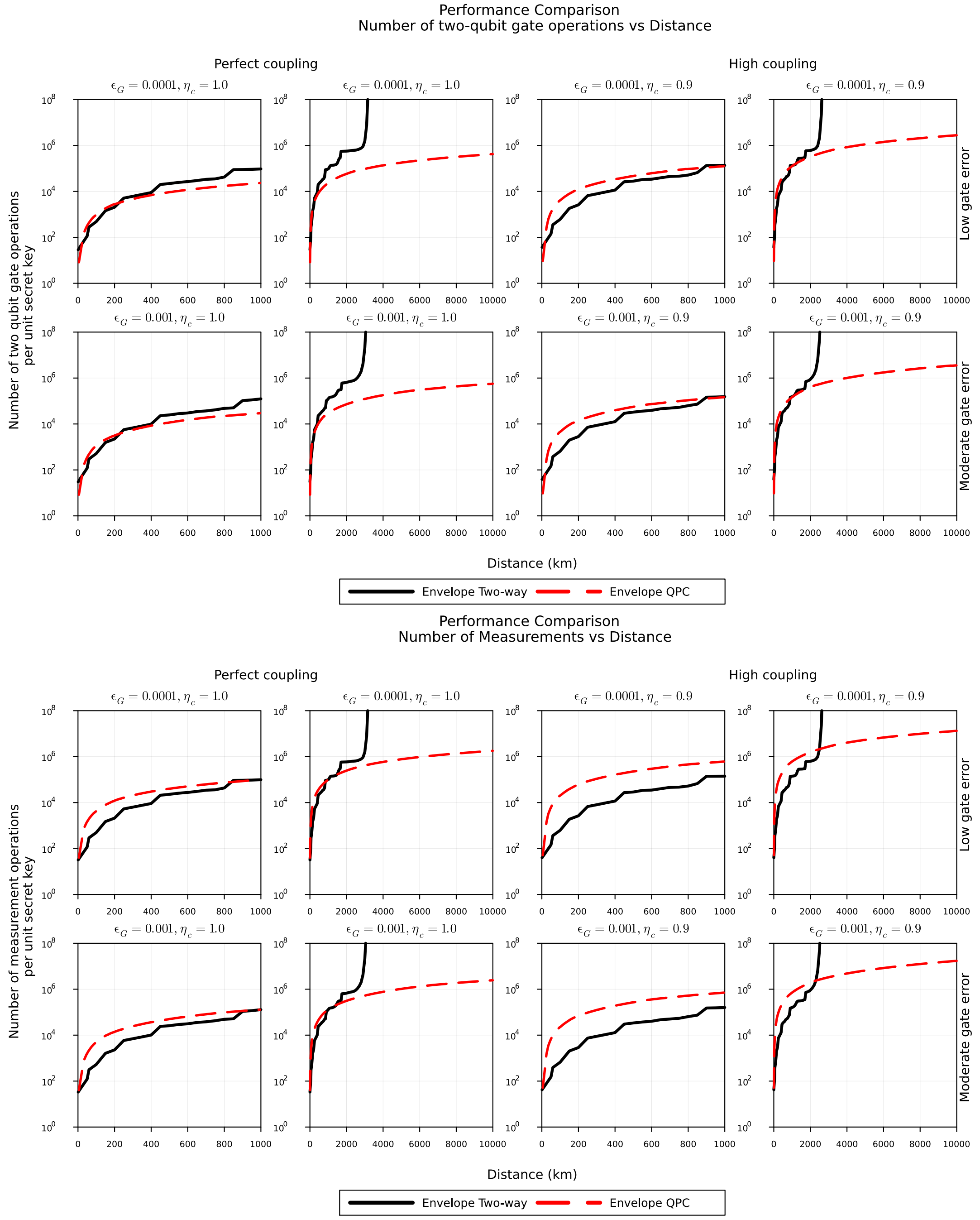

Figure 8: Number of (a) two-qubit gates and (b) measurement operations required per burst for each unit secret key delivered for one- and two-way repeater architectures. The red dashed line shows the number of repeaters required for the optimal Quantum Parity Code (QPC), and the black solid line is the envelope for the highest deliverable secret key rate for 'always distill at elementary link protocol' of the multiplexed two-way scheme (MTP) for any distance. To note, for QPCs, we have not considered gate operations required for state preparation or gate operations on ancilla qubits, and the estimation presented here is a lower bound.

4 Performance comparison of the SKR rule MTP with QPC with varying gate errors and coupling efficiencies

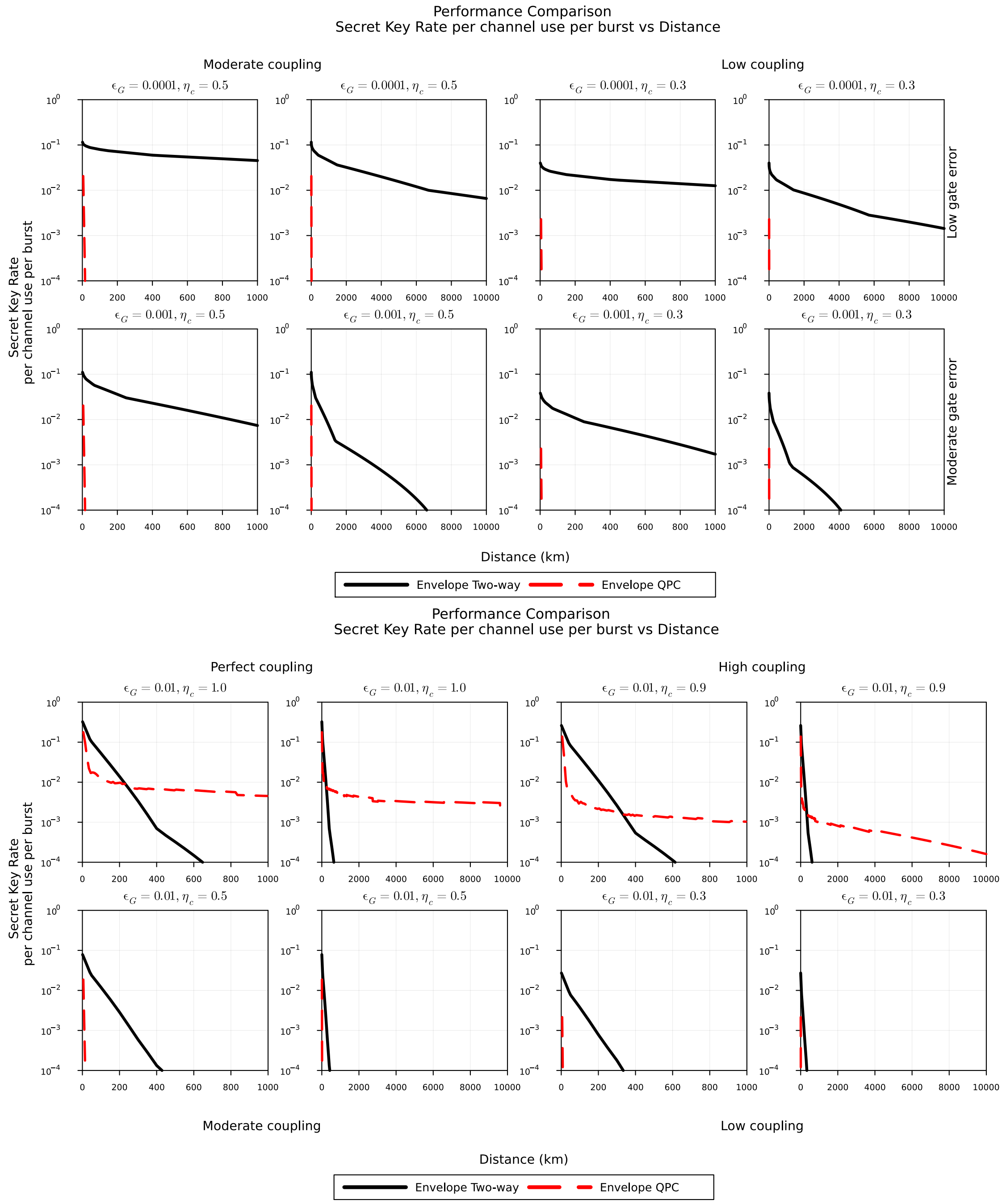

Figure 9: Performance comparison between QPC and MTP schemes using the secret-key rate as the metric for (a) moderate and low coupling $\eta_c \in \{0.5, 0.3\}$)for low and moderate gate errors ($\epsilon_G \in \{0.0001, 0.001\}$) (b)high gate errors $\epsilon_G = 0.01$ or 1% for four different coupling regimes ($\eta_c \in \{1, 0.9, 0.5, 0.3\}$). The red dashed line shows the performance by the optimal Quantum Parity Codes (QPC), and the black solid line is the envelope for the secret key rates for multiplexed two-way scheme (MTP). For each distance, a specific (n, m) QPC is chosen optimizing for total number of qubits required with the search parameters constrained to $n \leq 70, m \leq 20$. For the MTP, a maximum of 1024 multiplexed channels have been considered.