Comparing One- and Two-way Quantum Repeater Architectures Supplementary Materials

Prateek Mantri[1], Kenneth Goodenough[2], and Don Towsley[3]
{[1]pmantri, [2]kgoodenough, [3]towsley}@cs.umass.edu

Robert and Donna Manning College of Information and Computer Sciences,
University of Massachusetts, Amherst, MA, USA 01002

Supplementary Methods

This section outlines the models assumed for various processes and operations associated with the proposed Multiplexed Two-way Scheme. As mentioned in Methods section in the main text, we consider a linear network with each repeater station equipped with a large number of optically active memories or emitters.

A Elementary link generation

Emitters located at neighboring repeaters emit photons entangled with their state. These photons are then sent to a station located mid-way between the repeaters supporting an array of Bell State Analyzers (See Elementary Link Generation subsection in Methods section in the main text). These Bell state analysers perform probabilistic Bell state measurements, with the probability of successful generation of an elementary link given by

$$\pi_0 = \frac{1}{2}\eta_c^2 e^{-L_0/L_{att}}, \tag{1}$$

where η_c is the coupling efficiency, L_0 is the inter-repeater distance, and L_{att} is the attenuation length taken as 20 km in this manuscript.

B Fidelity

We model the generated quantum elementary link (represented as the two-qubit quantum state ρ) as a Bell-diagonal state. This state can be represented as a linear combination of the four Bell states -

$$\rho = a\left|\phi^+\right\rangle\left\langle\phi^+\right| + b\left|\phi^-\right\rangle\left\langle\phi^-\right| + c\left|\psi^+\right\rangle\left\langle\psi^+\right| + d\left|\psi^-\right\rangle\left\langle\psi^-\right| \ , \tag{2}$$

where $|\varphi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ are the four Bell states. As a shorthand, we represent this state as the state tuple (a, b, c, d) corresponding to the probabilities of each of the four Bell states. Fidelity of ρ is given by $F \equiv \langle\phi^+|\,\rho\,|\phi^+\rangle = a$.

C Gate operations

Local two-qubit gates, such as the CNOT gate, are characterised by the gate error parameter ϵ_G. This parameter indicates the probability that the gate operation will result into a maximally mixed state. Conversely, with probability $1-\epsilon_G$, the gate performs the intended operation correctly. This can be mathematically expressed as -

$$\mathcal{N}_{\tilde{U}_{ij}}(\rho) = (1-\epsilon_G)U_{ij}\rho U_{ij}^\dagger + \frac{\epsilon_G}{4}\mathrm{Tr}_{ij}[\rho] \otimes I_{ij}, \tag{3}$$

where U_{ij} represents the ideal two-qubit operation on qubits i and j, $\mathrm{Tr}_{ij}[\rho]$ denotes the partial trace over qubits i and j, and I_{ij} is the identity operator.

D Measurement operations

Measurement errors in qubits are described by the measurement error ξ, which quantifies the probability of an incorrect measurement outcome. The error models for projective measurements on the states $|0\rangle$ and $|1\rangle$ are given by-

$$P_0 = (1-\xi)|0\rangle\langle 0| + \xi|1\rangle\langle 1|, \tag{4}$$

$$P_1 = (1-\xi)|1\rangle\langle 1| + \xi|0\rangle\langle 0|. \tag{5}$$

To mitigate measurement errors, an ancillary qubit can be introduced and both the data qubit and the ancillary qubit can be measured. If the measurement outcomes differ, it is interpreted as a loss error on the qubit. Using the same argument forwarded in Muralidharan *et. al* [1], we assume the effective measurement error to be given by $\epsilon_G/4$, in case of a match of measurement outcomes. This is reasonable since the gate error rates considered range between 10^{-4} and 10^{-2}, making the contribution of measurement errors to the overall error rate to be minimal.

E Memory Decoherence

Quantum memories undergo decoherence with time. While this decoherence is commonly modelled to be either due to relaxing (T_1) or dephasing (T_2), we only include the effects of dephasing in our analysis. Because of decoherence, the state tuple (a, b, c, d) is updated in the following manner to $(a_{dec}, b_{dec}, c_{dec}, d_{dec})$, where

$$\begin{aligned} a_{dec} &= \lambda_{dec} a + (1-\lambda_{dec}) b \ , \\ b_{dec} &= \lambda_{dec} b + (1-\lambda_{dec}) a \ , \\ c_{dec} &= \lambda_{dec} c + (1-\lambda_{dec}) d \ , \\ d_{dec} &= \lambda_{dec} d + (1-\lambda_{dec}) c \ . \end{aligned} \tag{6}$$

Here $\lambda_{dec} = \frac{1+e^{-2t/T_2}}{2}$ [2], and t is the time that the state ρ is stored in memory.

F Distillation

For two links with state tuple - (a_1, b_1, c_1, d_1) and (a_2, b_2, c_2, d_2), the DEJMPS [1, 3] distillation protocol leads to the tuple (a, b, c, d) with a probability of success given by $p^{\uparrow}$

$$\begin{aligned} p^{\uparrow} = (1-\epsilon_G)^2\{&[\xi^2 + (1-\xi)^2][(a_1+d_1)(a_2+d_2) + (b_1+c_1)(c_2+b_2)] \\ &+ 2\xi(1-\xi)[(a_1+d_1)(b_2+c_2) + (b_1+c_1)(a_2+d_2)]\} + \frac{1}{2}[1-(1-\epsilon_G)^2] \end{aligned} \tag{7}$$

$$\begin{aligned} a &= \frac{1}{p^{\uparrow}}\{(1-\epsilon_G)^2[(\xi^2 + (1-\xi)^2](a_1a_2 + d_1d_2) + 2\xi(1-\xi)(a_1c_2 + d_1b_2)\} + \frac{1}{8}[1-(1-\epsilon_G)^2] \\ b &= \frac{1}{p^{\uparrow}}\{(1-\epsilon_G)^2[(\xi^2 + (1-\xi)^2](a_1d_2 + d_1a_2) + 2\xi(1-\xi)(a_1b_2 + d_1c_2)\} + \frac{1}{8}[1-(1-\epsilon_G)^2] \\ c &= \frac{1}{p^{\uparrow}}\{(1-\epsilon_G)^2[(\xi^2 + (1-\xi)^2](b_1b_2 + c_1c_2) + 2\xi(1-\xi)(b_1d_2 + c_1a_2)\} + \frac{1}{8}[1-(1-\epsilon_G)^2] \\ d &= \frac{1}{p^{\uparrow}}\{(1-\epsilon_G)^2[(\xi^2 + (1-\xi)^2](b_1c_2 + c_1b_2) + 2\xi(1-\xi)(b_1a_2 + c_1d_2)\} + \frac{1}{8}[1-(1-\epsilon_G)^2]. \end{aligned} \tag{8}$$

G Entanglement Swapping

Entanglement swapping is used in two-way quantum networks to extend the distance of entanglement. With imperfect CNOT operation and measurements, the state $\{a, b, c, d\}$ obtained from deterministically swapping the input pairs $\{a_1, b_1, c_1, d_1\}$ and $\{a_2, b_2, c_2, d_2\}$ is

$$\begin{aligned}
a &= (1-\epsilon_G)\{(1-\xi)^2(a_1a_2+b_1b_2+c_1c_2+d_1d_2)+\xi(1-\xi)[(a_1+d_1)(b_2+c_2)+(b_1+c_1)(a_2+d_2)] \\
&\quad +\xi^2(a_1d_2+d_1a_2+b_1c_2+c_1b_2)\}+\frac{\epsilon_G}{4} \\
b &= (1-\epsilon_G)\{(1-\xi)^2(a_1b_2+b_1a_2+c_1d_2+d_1c_2)+\xi(1-\xi)[(a_1+d_1)(a_2+d_2)+(b_1+c_1)(b_2+c_2)] \\
&\quad +\xi^2(a_1c_2+c_1a_2+b_1d_2+d_1b_2)\}+\frac{\epsilon_G}{4} \\
c &= (1-\epsilon_G)\{(1-\xi)^2(a_1c_2+c_1a_2+b_1d_2+d_1b_2)+\xi(1-\xi)[(a_1+d_1)(a_2+d_2)+(b_1+c_1)(b_2+c_2)] \\
&\quad +\xi^2(a_1b_2+b_1a_2+c_1d_2+d_1c_2)\}+\frac{\epsilon_G}{4} \\
d &= (1-\epsilon_G)\{(1-\xi)^2(a_1d_2+d_1a_2+c_1b_2+b_1c_2)+\xi(1-\xi)[(a_1+d_1)(b_2+c_2)+(b_1+c_1)(a_2+d_2)] \\
&\quad +\xi^2(a_1a_2+b_1b_2+c_1c_2+d_1d_2)\}+\frac{\epsilon_G}{4}\ . \qquad (9)
\end{aligned}$$

H Secret-key rate

The secure key generation rate, R_{secret} (sbit/s), can be written as

$$R_{secret} = P_{succ} \cdot r_{secure} \cdot \frac{1}{t_{max}}\ , \qquad (10)$$

where P_{succ} is the overall success probability of the protocol, t_{max} is the maximum time taken to generate a Bell pair between the two parties, and r_{secure} is the asymptotic secure fraction in the fully asymmetric version using the one-way BB84 protocol [4],

$$r_{secure}(\rho) = \max[1 - h(Q_X) - h(Q_Z)), 0]\ , \qquad (11)$$

where $\{Q_{X/Z}\}$ is the quantum bit error rate (QBER) for phase and bit flips, and can be calculated from the density matrix of the entangled state ρ shared by Alice and Bob in the end. Here,

$$h(Q_{\{X/Z\}}) = -Q_{\{X/Z\}} \log_2 Q_{\{X/Z\}} - (1 - Q_{\{X/Z\}}) \log_2(1 - Q_{\{X/Z\}})$$

is the binary entropy function. In Muralidharan et al. [1], an average for quantum bit error rate is taken with $Q = \frac{Q_X+Q_Z}{2}$, and secure rate is approximated as $r_{secure} = \max[1 - 2h(Q), 0]$. For our analysis, we assume pipelining, and allow for an arbitrary number of bursts in unit time-frame. For this we define the quantity Secret-key rate per burst as

$$SKR = \mathbb{E}(Y) \cdot r_{secure}, \qquad (12)$$

where Y is the number of Bell pairs shared between two parties. Since QPC and MTP use different number of elementary channels, we further modify this quantity to define the metric of Secret-key rate per channel use per burst-

$$SKR \text{ (per channel use) } = \frac{\mathbb{E}(Y) \cdot r_{secure}}{M}, \qquad (13)$$

where M denote the number of multiplexed channels available at each elementary link, and in the case of (n, m) QPC, M is the total number of physical qubits encoding one logical qubit i.e. $M = nm$.

I Recursive formulation for a general n-to-k distillation protocol

We can reconfigure the recursive formulation outlined in the main text for a distillation protocol based on the Steane code, equation (8) from the main text can be updated to —

$$
\begin{aligned}
q'_{i,k} &= P(Y_i = k | \text{ no reset at levels } 0, 1, \ldots, i) \\
&= \begin{cases} \sum_{j=7k}^{M_i} p'_{i,j} \binom{\lfloor j/7 \rfloor}{k} d_i^k \overline{d}_i^{\lfloor j/7 \rfloor - k} & , \quad \mathcal{D}_i = 1 \\ p'_{i,k} & , \quad \mathcal{D}_i = 0 \end{cases}, \quad \forall k \in \{0, 1, \ldots, \lfloor M_i/7 \rfloor\},
\end{aligned}
\tag{14}
$$

where $M_i = M/7^{\sum_{i=0}^{i} \mathcal{D}_{i-1}}$, $M = m \cdot 7^{n+1}$, and $m \in \mathbb{Z}^+$. For a more general n'-to-k' protocol we can define $q'_{i,k}$ as,

$$
\begin{aligned}
q'_{i,k} &= P(Y_i = k | \text{ no reset at levels } 0, 1, \ldots, i) \\
&= \begin{cases} \sum_{j=k \cdot \lceil (n'/k') \rceil}^{M_i} p'_{i,j} \binom{\lfloor j/\lceil (n'/k') \rceil \rfloor}{k} d_i^k \overline{d}_i^{\lfloor j/\lceil (n'/k') \rceil \rfloor - k} & , \quad \mathcal{D}_i = 1 \\ p'_{i,k} & , \quad \mathcal{D}_i = 0 \end{cases}, \quad \forall k \in \{0, 1, \ldots, \lfloor M_i/\lceil n'/k' \rceil \rfloor\}
\end{aligned}
\tag{15}
$$

where $M_i = M/(\lceil n'/k' \rceil)^{\sum_{i=0}^{i} \mathcal{D}_{i-1}}$, $M = m \cdot \lceil n'/k' \rceil^{n+1}$, and $m \in \mathbb{Z}^+$.
Equations (7), (9), (10), and (11) from the main text will remain the same as the DEJMPS case.

Supplementary Note 1

A Description of protocols

In this section we consider four distillation policies for the multiplexed two-way (MTP) protocol,

1. **SKR rule based distillation policy:** Here the decision to distill is based on Secret Key Rate given by equation (12) from the main text. The expected number of bell pairs at any level are computed using equation (13) in the main text.

2. **Distillation based on Fidelity Threshold:** In this if the fidelity F_i at any level i is less than the threshold fidelity F_{th}, we perform a single round of distillation i.e. $F_{th} \underset{\mathcal{D}_i=0}{\overset{\mathcal{D}_i=1}{\gtrless}} F_i, \forall i \in \{0, \cdots, n-1\}$. To note, similar to the SKR rule, no distillation is performed at the last level.

3. **Always distill at elementary link level policy:** 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.

4. **Always distill at all nesting levels policy:** 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.

B 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 ($\eta_c = 0.9$)

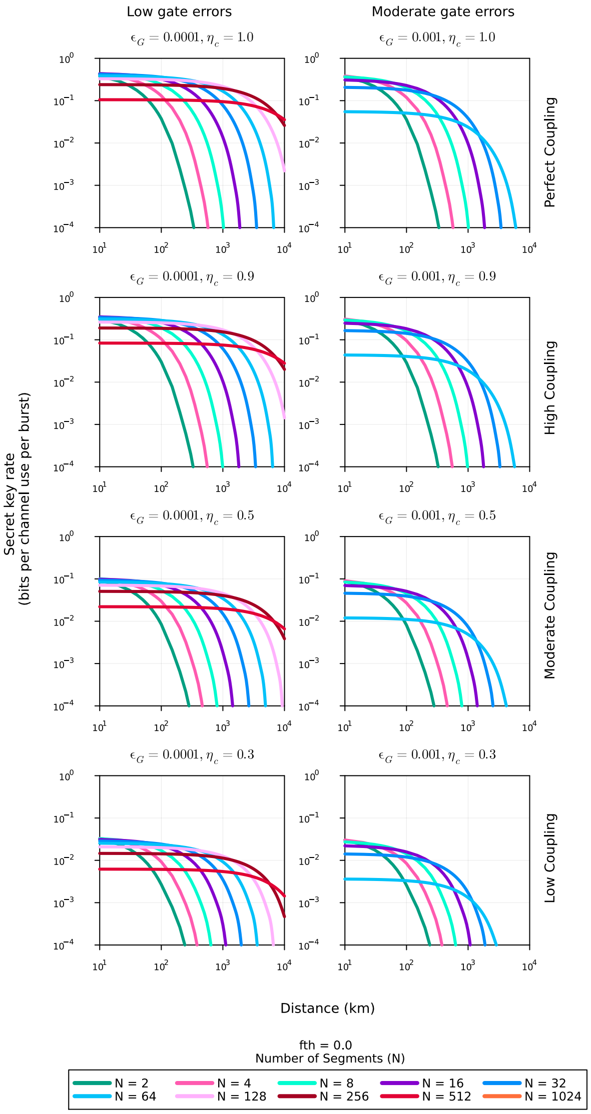
3. Moderate gate errors ($\epsilon_G = 10^{-3}$) and perfect coupling ($\eta_c = 1.0$)

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

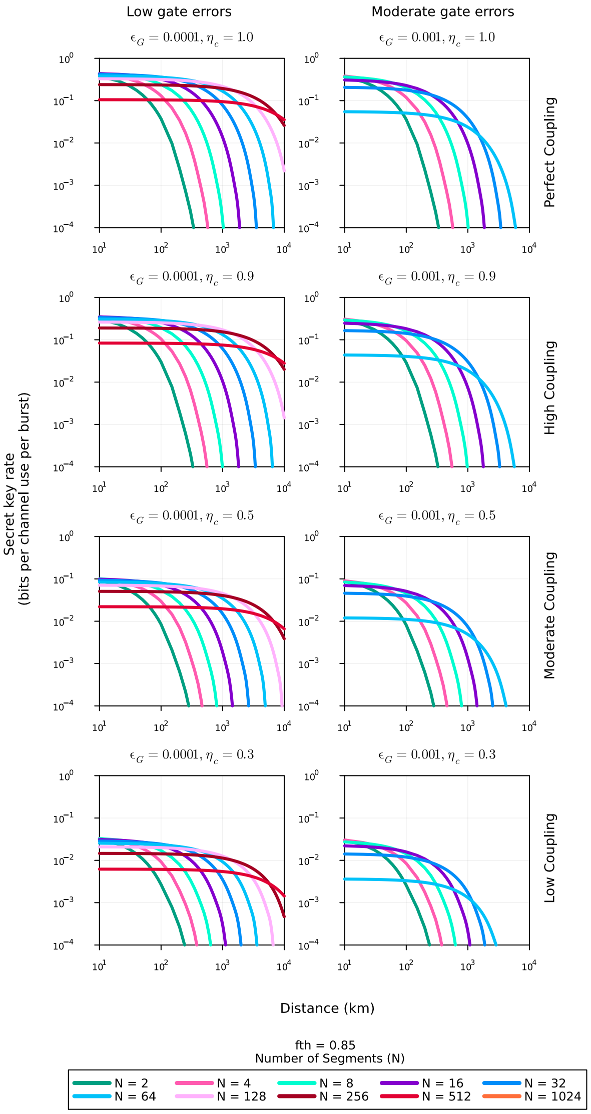
Additionally, for the SKR rule, we have included the performance plots for the different coupling and higher gate errors that have not been covered in the main text (See Performance Evaluation subsection in Results section in the main text).

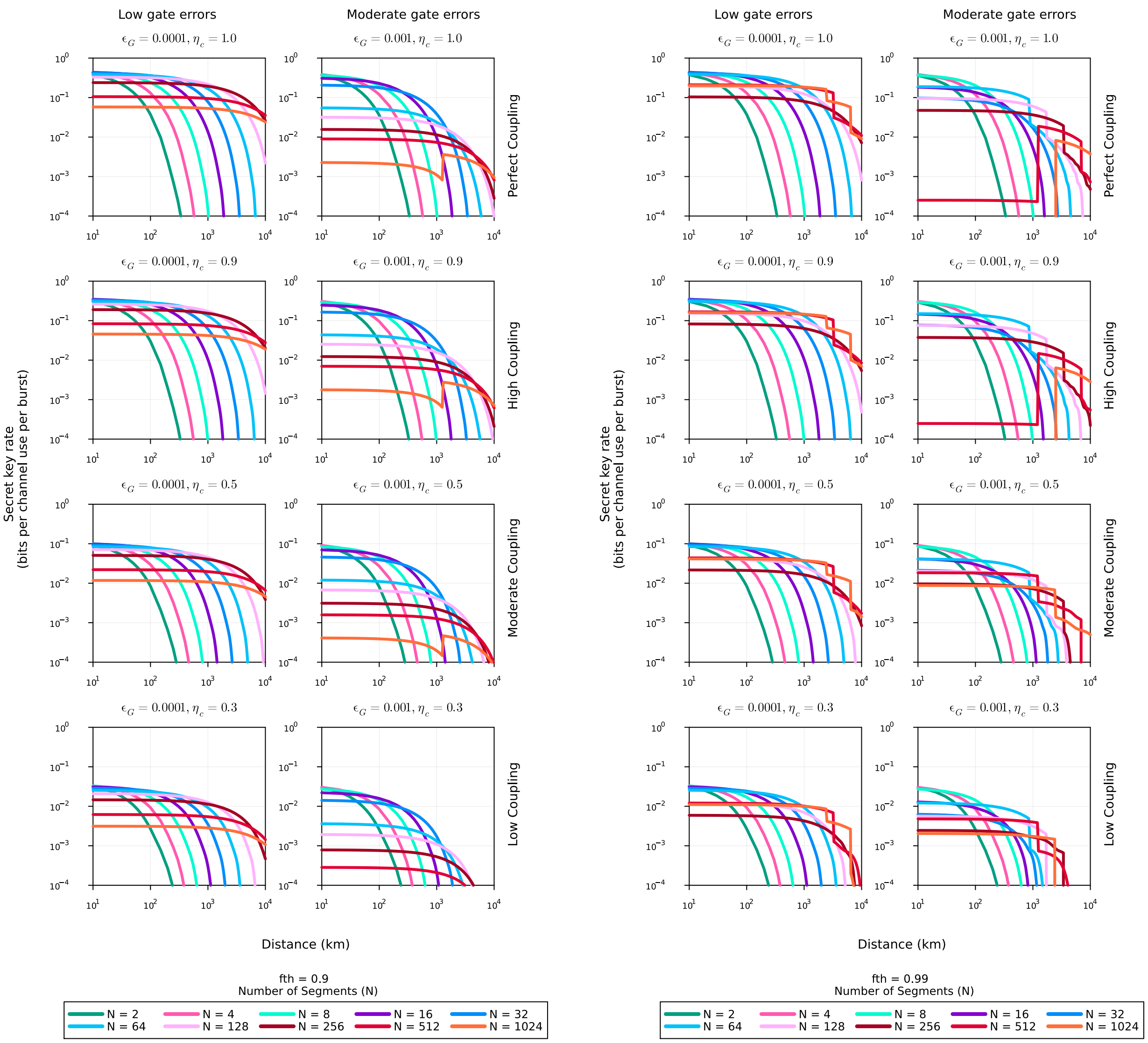
C Results

(a) $F_{th} = 0.0$ - No Distillation At Any Level



(b) $F_{th} = 0.8$



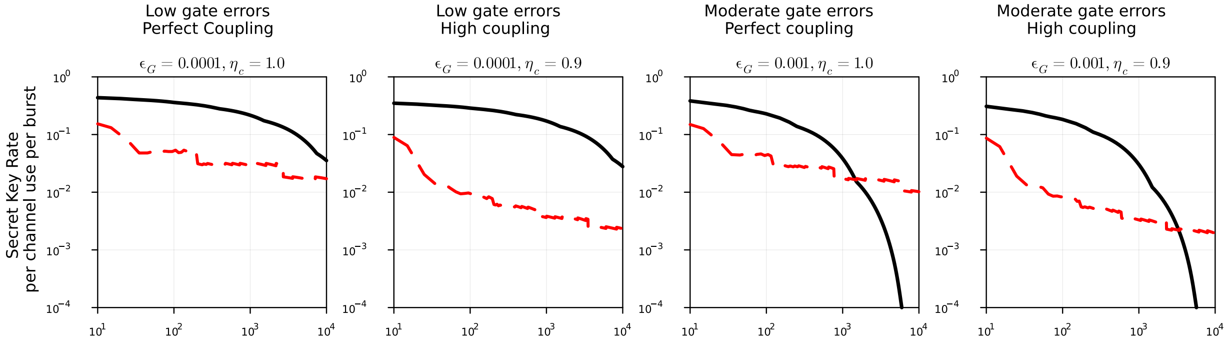


(c) $F_{th} = 0.9$

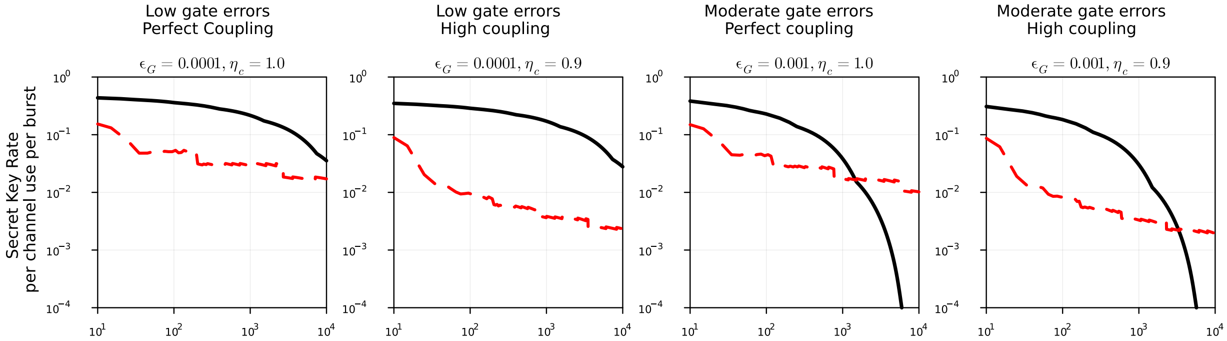
(d) $F_{th} = 0.99$

Supplementary Figure 1: Performance of two-way multiplexed protocol with distance using secret key rate as the metric for **a single round per nesting level distillation policy based on fidelity thresholds**. The number of segments are shown in different colors and denoted by N with different $F_{th} \in \{0, 0.8, 0.9, 0.99\}$. The plots shown in the odd column (columns 1 and 3) consider a low gate error scenario with a gate error rate (ϵ_G) of 10^{-4} or 0.01%, and the plots in the even columns 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 ($\eta_c \in \{1, 0.9, 0.5, 0.3\}$). In this setup we have used the protocol based on fidelity thresholds to inform the distillation decision making with a maximum of one round of distillation allowed at any level of nesting. Also, similar to all the MTP schemes considered, no distillation is performed at the end level.

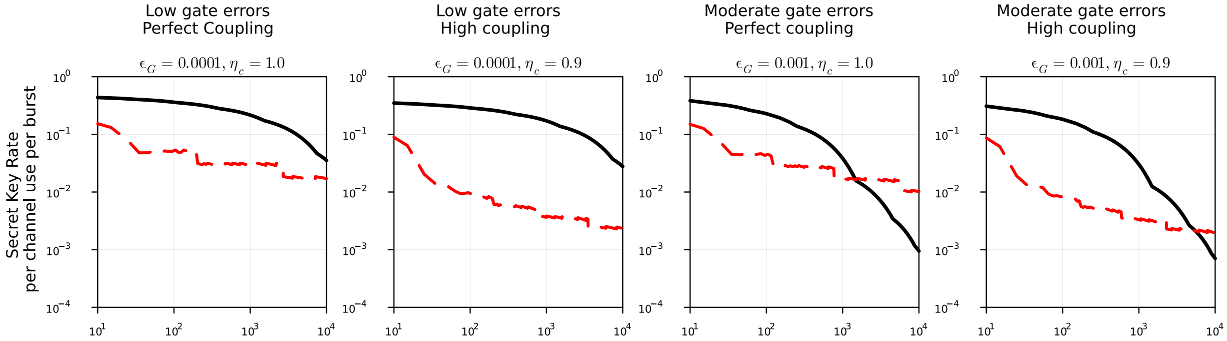
(a) $F_{th} = 0.0$ - No Distillation At Any Level

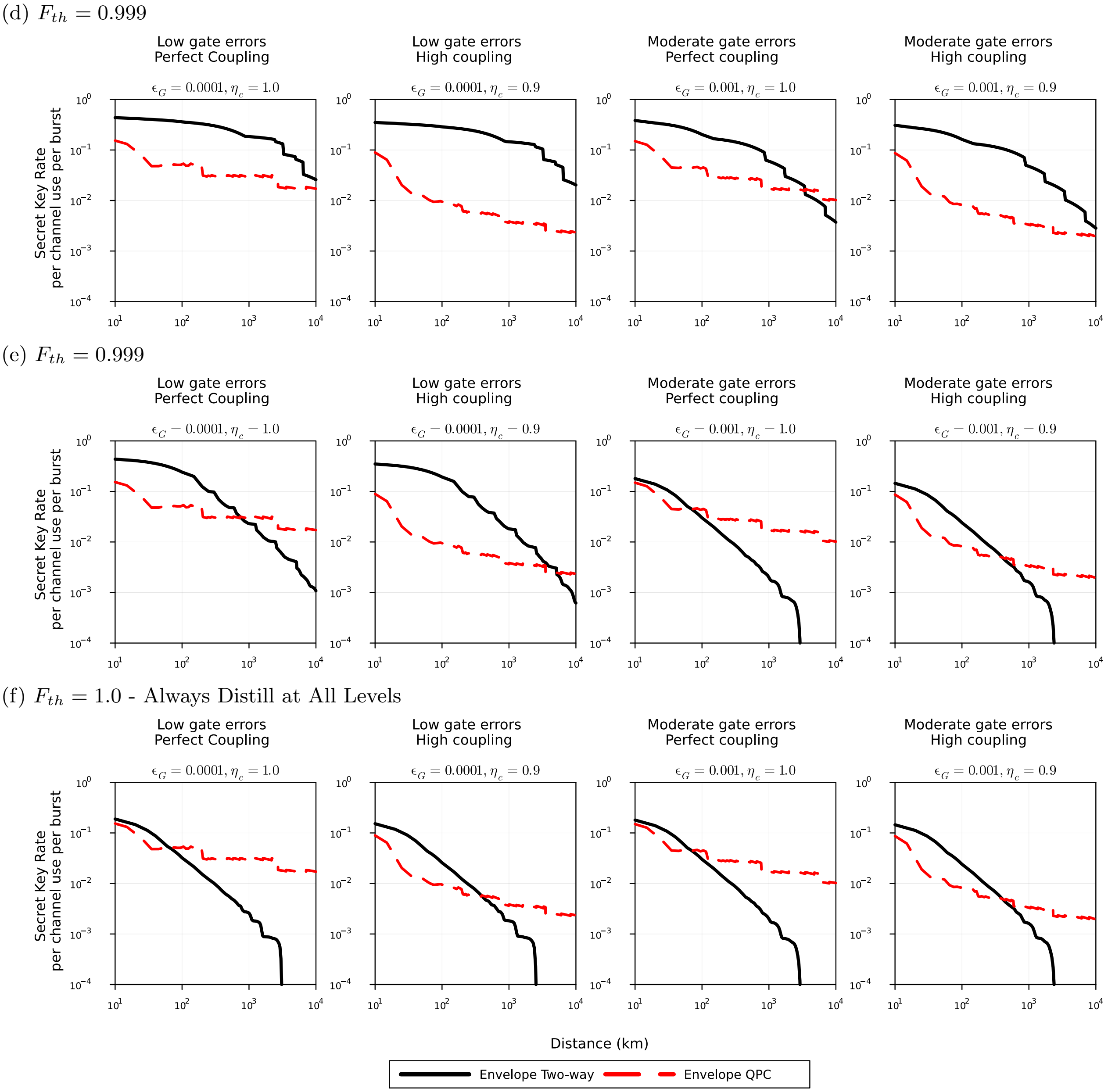


(b) $F_{th} = 0.85$



(c) $F_{th} = 0.9$



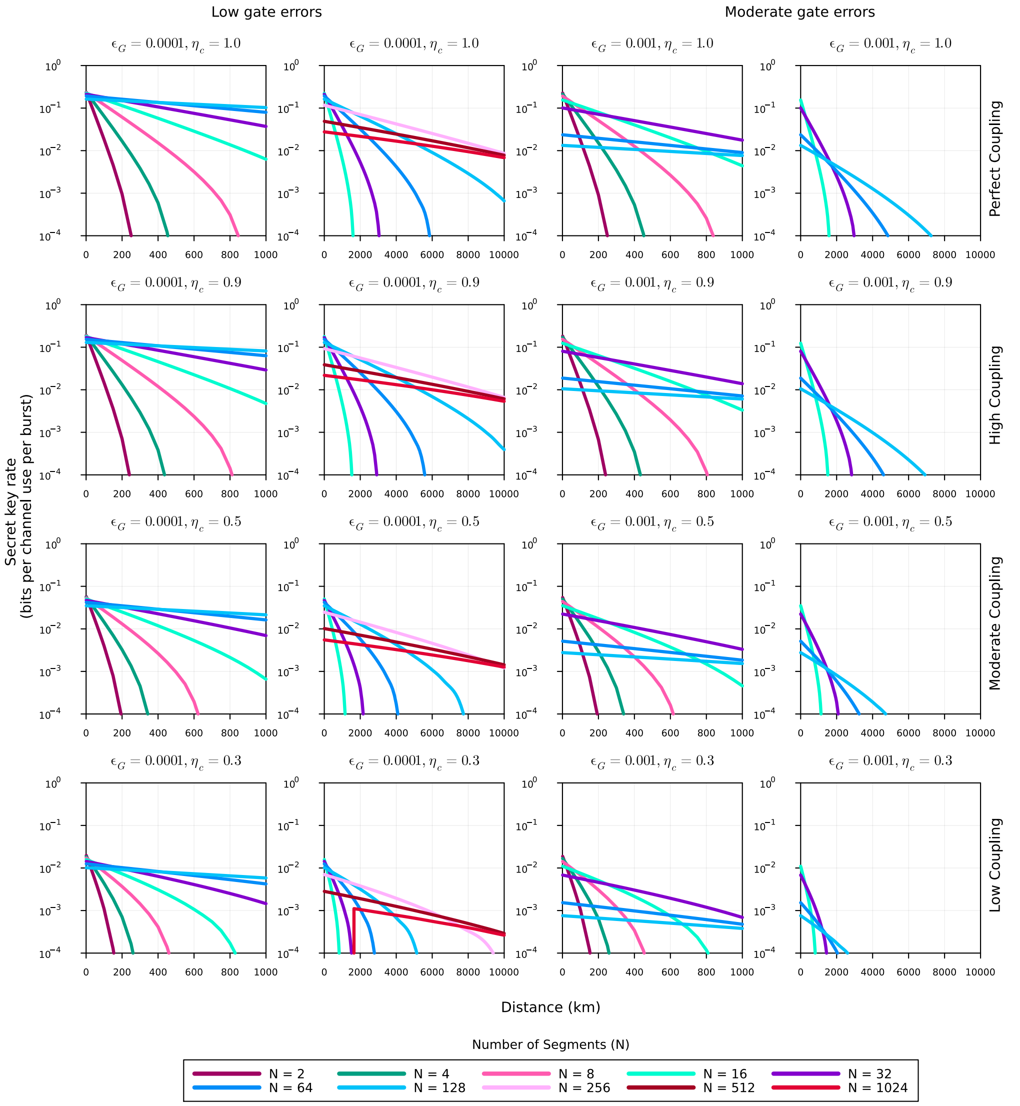


(d) $F_{th} = 0.999$

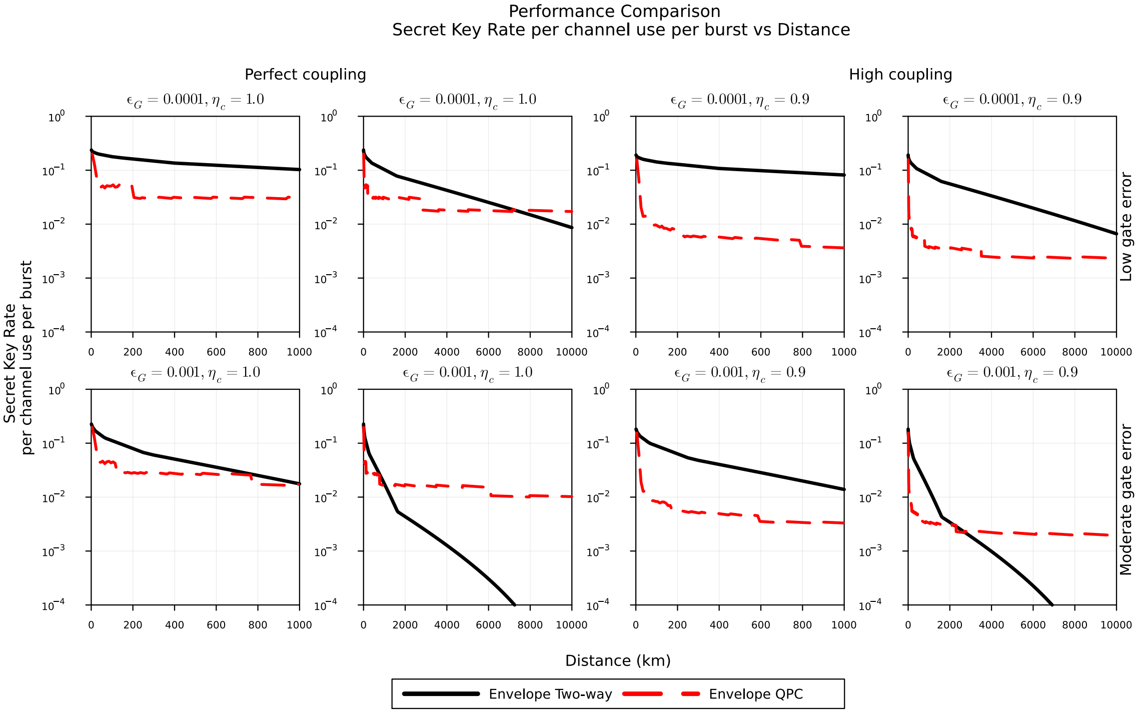
(e) $F_{th} = 0.999$

(f) $F_{th} = 1.0$ - Always Distill at All Levels

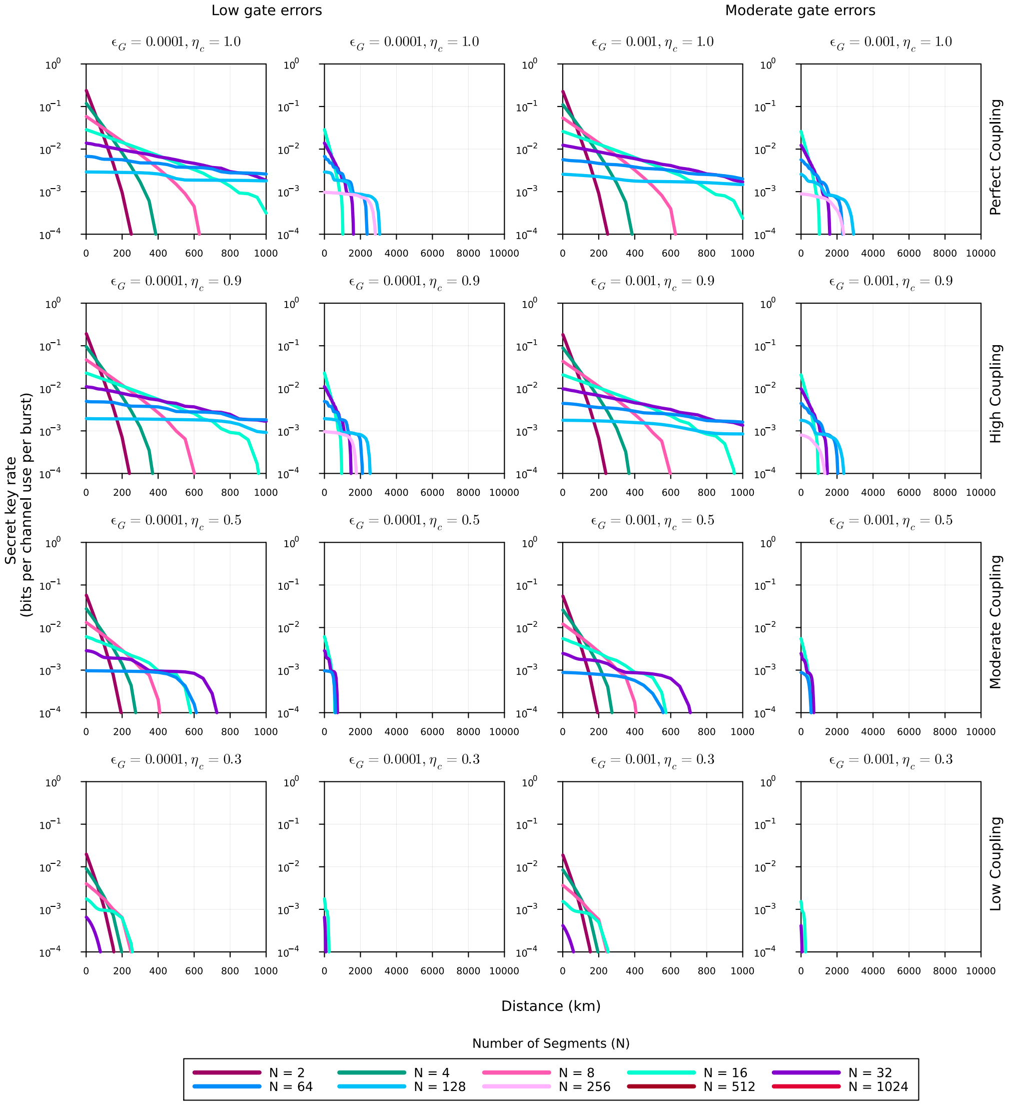
Supplementary Figure 2: Performance comparison between one-way and two-way schemes using the secret-key rate as the metric for **a single round per nesting level distillation policy based on fidelity thresholds**. The red dashed line shows the performance by the optimal Quantum Parity Codes (QPC), and 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 this flavor of the MTP, a maximum of 1024 multiplexed channels have been considered. 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 when the fidelity of the state after swap is lesser than a threshold fidelity F_{th}. Also, similar to all the MTP schemes considered, no distillation is performed at the end level.



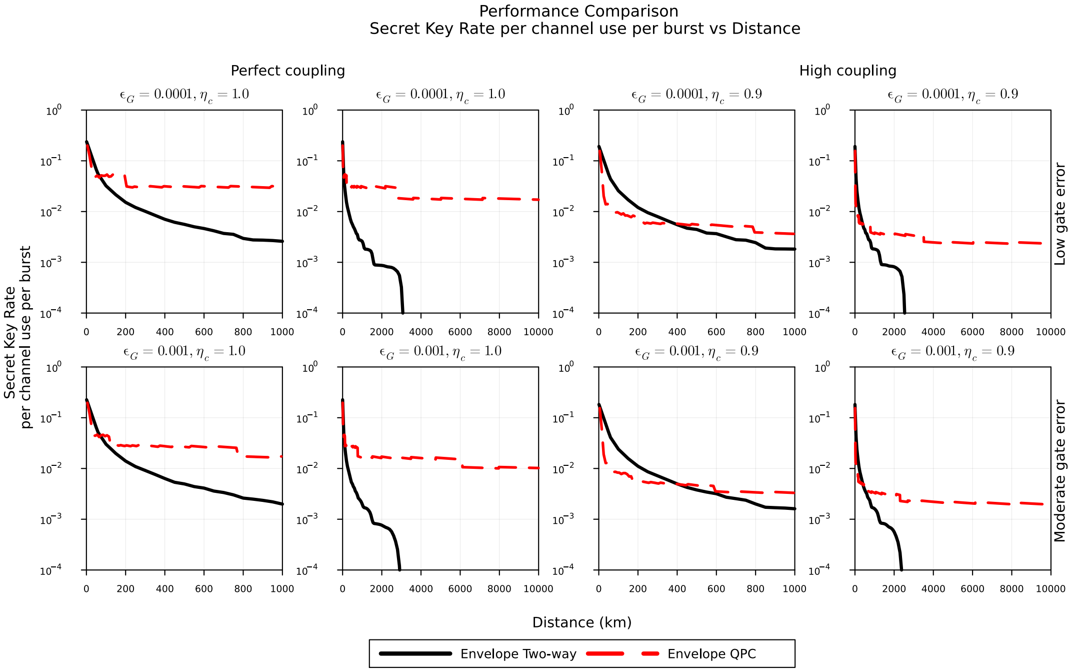
Supplementary Figure 3: Performance of two-way multiplexed protocol with distance using secret key rate as the metric for the **always distill at elementary link policy**. The number of segments are shown in different colors and denoted by N. The left hand side plots consider a low gate error scenario 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.



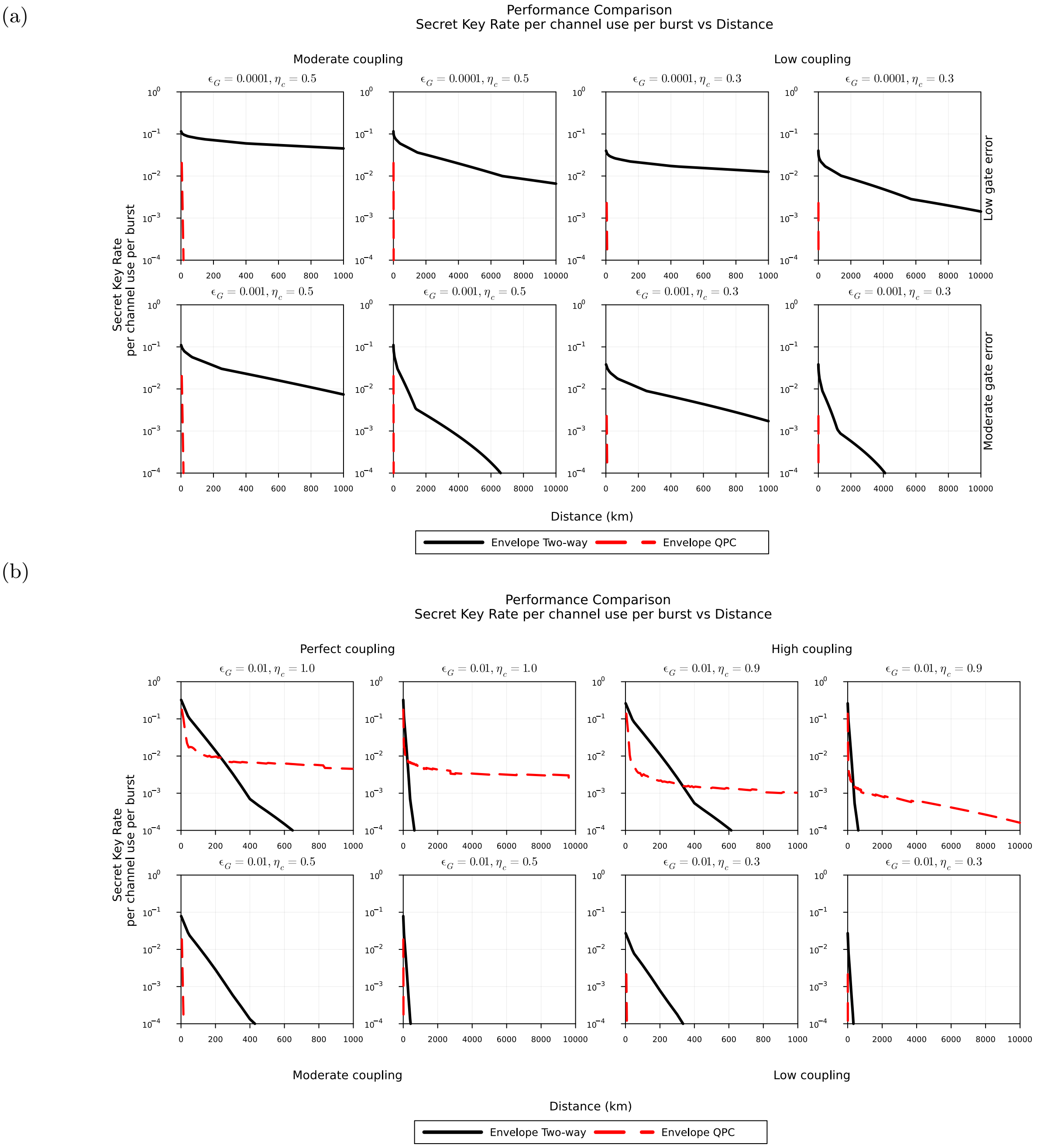
Supplementary Figure 4: Performance comparison between one-way and two-way schemes using the secret-key rate as the metric for the **always distill at elementary link policy**. The red dashed line shows the performance by the optimal Quantum Parity Codes (QPC), and the black solid line is the envelope 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.



Supplementary Figure 5: Performance of two-way multiplexed protocol with distance using secret key rate as the metric for the **always distill at all nesting levels policy**. 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.



Supplementary Figure 6: Performance comparison between one-way and two-way schemes using the secret-key rate as the metric for the **always distill at all nesting levels policy**. 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.



Supplementary Figure 7: **Performance comparison of the SKR rule MTP with QPC with varying gate errors and coupling efficiencies**. Here the the secret-key rate has been used as a metric for comparing performance differences at (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.

Supplementary References

1. Muralidharan, S. *et al.* Optimal architectures for long distance quantum communication. en. *Scientific Reports* **6,** 20463. ISSN: 2045-2322. http://www.nature.com/articles/srep20463 (2022) (Apr. 2016).

2. Munro, W. J., Azuma, K., Tamaki, K. & Nemoto, K. Inside Quantum Repeaters. *IEEE Journal of Selected Topics in Quantum Electronics* **21.** Conference Name: IEEE Journal of Selected Topics in Quantum Electronics, 78–90. ISSN: 1558-4542. https://ieeexplore.ieee.org/document/7010905 (2024) (May 2015).

3. Deutsch, D. *et al.* Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. en. *Physical Review Letters* **77,** 2818–2821. ISSN: 0031-9007, 1079-7114. https://link.aps.org/doi/10.1103/PhysRevLett.77.2818 (2024) (Sept. 1996).

4. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84* **560,** 7–11. ISSN: 0304-3975. https://www.sciencedirect.com/science/article/pii/S0304397514004241 (2024) (Dec. 2014).