Design of a Quantum-Repeater using Quantum-Circuits and Benchmarking its Performance on an IBM Quantum-Computer

Preprint · June 2019

DOI: 10.13140/RG.2.2.27719.14249

2 authors:

Sowmitra Das
BRAC University

Md. Saifur Rahman
Bangladesh University of Engineering and Technology

Design of a Quantum-Repeater using Quantum-Circuits and Benchmarking its Performance on an IBM Quantum-Computer

Sowmitra Das*, Md. Saifur Rahman† and Mahbub Alam Majumdar‡

***Abstract*—Quantum communication relies on the existence of entanglement between two nodes of a network. Since, entanglement can only be produced using local quantum operations, distribution of parts of this entangled system between different nodes becomes necessary. However, due to the extremely fragile nature of entanglement and the presence of losses in the communication channel, the direct distribution of entanglement over large distances is nearly impossible. Quantum repeaters have been proposed to solve this problem. These enable one to establish long-range entanglement by dividing the link into smaller parts, creating entanglement between each part and connecting them up to form the full link. As researchers race to establish entanglement over larger and larger distances, it becomes essential to gauge the performance and robustness of the different protocols that go into designing a quantum repeater, before deploying them in real life. Present day noisy quantum computers are ideal for this task as they can emulate the noisy environment in a quantum communication channel and provide a benchmark for how the protocols will perform on real-life hardware. In this paper, we report the circuit-level implementation of the complete architecture of a Quantum Repeater. All the protocols of the repeater have been bench-marked on IBM Q, the world's first publicly available cloud quantum computer. The results of our experiment provide a measure for the fidelity of entanglement current repeaters can establish. In addition, the repeater protocol provides a robust benchmark for the current state-of-the-art of quantum computing hardware.**

***Index Terms*—Quantum Communication, Quantum Circuits, IBMQ, Entanglement Swapping, Entanglement Purification, Quantum Privacy Amplification**

I. Introduction

QUANTUM communication is the method of transmitting information signals by exploiting the the principles of quantum mechanics [1], [2]. It enables novel communication paradigms such as quantum teleportation [3], superdense coding [4], unbreakable cryptography [5] and information-theoretic security of key distribution [6] - all of which have no classical counterpart. These protocols require the existence of entanglement between the transmitting and receiving parties. Photonic channels have proved to be a reliable medium for communicating classical signals over long distances. However, quantum entanglement is an extremely fragile resource, and, the smallest amount of noise (thermal or otherwise) in the environment can render them useless. The attenuation length of classical photonic channels for these quantum signals is few kilometers at best [7], [8]. As a result, it is nearly impossible to transmit entangled photons over large distances preserving their fidelity. Classical repeaters tackle this issue this by simply amplifying, or by measuring and regenerating, the input signal. But, the no-cloning theorem forbids the amplification of quantum signals [9], [10], and, decoherence does not allow us to measure quantum systems without destroying their information content [11].

Quantum repeaters have been proposed to solve this problem [12]. The idea behind them is to divide the entire link into many small segments - the length of each segment being less than the attenuation length of the channel. Next, entanglement is established between the endpoints of each of these smaller links by the direct transmission of photons. Then, by using the entanglement swapping protocol, all of these smaller links are connected up to establish the large-scale link. At each successive step of this process, there might be loss of fidelity due to noise or imperfections in the operating hardware. So, at each step, the entangled links are "purified" to increase the fidelity of entanglement between the nodes [13]. By repeating this protocol a sufficient number of times, we can theoretically establish a large-scale entangled link of arbitrarily high fidelity.

These ideas are already being tested on the field as researchers around the globe race to establish entanglement over larger and larger distances, spanning thousands of kilometres. Significant progress has been made in recent years [14], [15], [16], [17]. However, it still remains a difficult problem for real-life deployment, due to the extremely noisy and unpredictable nature of the quantum channel, the sensitivity of quantum signals to external influence, and, the stringent conditions and high-precision instruments required to design the systems. As we enter the Noisy Intermediate-Scale Quantum (NISQ) era, quantum communication technologies are poised to disrupt and revolutionize the entire communication infrastructure [18]. So, it is more important than ever, that we can predict how these protocols and systems will behave in real quantum environments. This will enable us to test the robustness of our algorithms before committing resources to deploy them in real life. Unfortunately, it is exceedingly difficult to model a quantum channel by using classical resources or hardware. This approach requires enormous amounts of computational resources, and, for larger systems, can fall short of exactly capturing the quantum-mechanical behaviour of the channel altogether - even if it is possible at all. So, instead of simu-

*,‡Department of Computer Science and Engineering, BRAC University, Dhaka-1212, Bangladesh.

†Department of Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology, Dhaka-1205, Bangladesh.

E-mail: *sowmitra.das@bracu.ac.bd, †saifur@eee.buet.ac.bd, ‡majumdar@bracu.buet.ac.bd

lating these channels and protocols classically, the best way forward would be to use actual quantum-mechanical hardware to emulate their effects [19].

A significant stepping stone in this direction was the release of IBMQ - world's first Quantum Computer with open access to the general public via the cloud - which ensued the start of the NISQ era [20]. With the IBMQ, researchers from across the globe can run experiments on its platform by designing circuits using IBM's Quantum Information Science toolKIT (QISKIT) [21]. The noisy hardware of IBMQ can perfectly emulate the conditions encountered in real-life quantum systems, particularly a quantum communication channel. Thus, they are the perfect candidates to to gauge the performance of current quantum communication protocols, and can be a useful guide for further research to make these protocols as robust as possible to real-life scenarios. With this end in view, we move to implement the complete end-to-end architecture of a Quantum Repeater on an IBM Quantum Computer.

A similar demonstration of this scheme has been given by Behera *et al*. in [22]. However, they have performed limited experiments in this regard, showing the results of entanglement swapping on 2 pairs of qubits only. In quantum-repeaters, entanglement-swapping has to be performed on multiple pairs of qubits successively in a nested fashion. As a result, hardware errors might accumulate in qubits impacting their fidelity. So, performing the entanglement-swapping protocol only one time likely doesn't give representative results of a real quantum repeater. In addition, they have also introduced a quantum error-correction code to purify the entangled-qubits by using Controlled-NOT (CNOT) operations on them. This approach is not suitable for large-scale quantum networks since CNOT, being a local-operation, cannot be performed on qubits separated by a large distance in space. In addition, they report that, the code can only correct 2 specific types of errors - namely, bit flip and phase-change - and, that too if the entangled qubits start out are in a pure-state. For more general types of errors in a quantum-communication channel, and, for qubits starting out in a mixed-state, their code fails to increase the fidelity of entanglement. For communication networks, this can be solved by condensing multiple low-fidelity entangled pairs into one high-fidelity pair by using an entanglement-distillation protocol. We demonstrate this general approach of building a quantum-repeater in our experiments.

Finally, we not only demonstrate a complete circuit-level implementation of a Quantum Repeater, but the result of our experiments also sheds light on the performance and accuracy of current quantum hardware. Zhukov *et al*. [23] have proposed that quantum communication protocols can serve as a deep benchmark for quantum computers. In contrast to generic protocols like superdense coding and quantum teleportation, which require only a few gate operations, the complete architecture of a Quantum Repeater uses multiple sub-protocols and stresses every physical aspect of the hardware platform which is running it. As a result, the quantum-repeater protocol can serve as a much more revealing benchmark compared to other protocols. This will offer us several metrics reflecting the real-life performance of Quantum Repeaters, and, help us evaluate the hardware limitations of current state-of-the-art noisy quantum computers.

The following sections of this paper are organised as follows. Section II introduces the basics of Quantum Circuits and how to design circuits for Quantum Computing Hardware. The basic protocols of Quantum Communication, for which entanglement-distribution is a key step, are shown next in Section III. Then, we move on to designing the fundamental Quantum Repeater architecture in Section IV, which includes the entanglement-distribution, entanglement swapping and entanglement purification protocols. In section V, we report the results of our experiments on the IBMQ platform, as well as simulation results with noise models for comparison. Finally, we explore the future directions of our research in Section VI with discussions on how to improve the yield and accuracy of the protocol even further.

II. Quantum Circuits

A. Qubits and 1-Qubit Gates

The fundamental building-block of a Quantum Circuit is the 'Qubit'. It is a two-dimensional quantum system with orthonormal basis-states $|0\rangle$ and $|1\rangle$ (known as the Computational Basis) [24]. The state $|\psi\rangle$ of a system can be any superposition of the basis states, which can be expressed as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

where, α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. The last equality asserts that, the states of a qubit are essentially vectors in a complex Hilbert Space, and, the whole machinery of linear algebra may be used in their manipulations. The orthonormal basis states might, for example, be the ground state $|g\rangle$ and an excited state $|e\rangle$ of a matter system or the horizontally polarised state $|H\rangle$ and vertically polarised state $|V\rangle$ of a single-photon system. In the context of a Quantum-Computing system, a collection of qubits form a *Quantum Register*, whereas, a collection of classical bits form a *Classical Register* [25].

Qubits may be manipulated by using *Operators*, which are represented as matrices. Operators which preserve the normalization of a state are called *Unitary Operators*. At the circuit-level, unitary operators are implemented by using Quantum Logic-Gates, or simply, Quantum-Gates. The prototypical quantum gates are the Pauli Gates X, Y, Z, the Hadamard Gate H and the Phase-Shift Gate R_θ [26]. Their matrix-representations are given below and circuit symbols are shown in Fig. 1.

$$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \qquad Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \qquad R_\theta = \begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix}$$

B. Ebits and 2-Qubit Gates

Two qubits A and B may exist in a tensor product-state $|\psi\rangle_A \otimes |\phi\rangle_B$, or written simply as $|\psi\rangle_A |\phi\rangle_B$, so that each qubit may be assigned an individual state vector $|\psi\rangle$ or $|\phi\rangle$. But, the

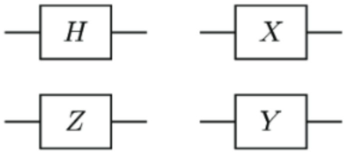


Fig. 1: Schematic Symbols for Quantum Logic Gates (in clockwise order) - Hadamard Gate, Pauli X (Not) Gate, Pauli Y Gate, Pauli Z Gate.

remarkable aspect of Quantum Mechanics is the existence of *Entanglement* between 2 qubits, where, the qubits may be in a superposition of product-states, but, separate state-vectors can not be assigned to them. The prototypical entangled states of a two-qubit system AB are the maximally entangled Bell-States, $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$, which are expressed in terms of the computational basis states as follows:

$$\left|\Phi^{\pm}\right\rangle_{AB} = \left(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B\right)/\sqrt{2}$$

$$\left|\Psi^{\pm}\right\rangle_{AB} = \left(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B\right)/\sqrt{2}$$

Two qubits in a Bell-State are also known as a Bell-Pair [27] or an EPR (Einstein-Podolsky-Rosen) Pair [28].

The Bell-States may be prepared by using the two-qubit Controlled-NOT (CNOT) Gate. The CNOT Gate flips the state of the target qubit ($|0\rangle$ to $|1\rangle$, or, $|1\rangle$ to $|0\rangle$) if the state of the control qubit is $|1\rangle$, and, it does nothing if the state of the control qubit is $|0\rangle$. If the control qubit is in a superposition state, the control and target qubits become entangled at the output of the gate. So, the CNOT Gate is a mechanism to entangle two qubits. Two qubits which are entangled in this way are called 'Entangled Bits' or 'Ebits' [25], [29].

The map of the CNOT Gate is shown as follows:

$$|a\rangle_{\text{control}} |b\rangle_{\text{target}} \xrightarrow{\text{CNOT}} |a\rangle_{\text{control}} |a \oplus b\rangle_{\text{target}}$$

where, $a, b \in \{0, 1\}$, and, $\oplus$ is the XOR operation.

Another example of a two-qubit gate is the SWAP gate, which exchanges the contents of the target and control qubit.

$$|\psi\rangle_{\text{control}} |\phi\rangle_{\text{target}} \xrightarrow{\text{SWAP}} |\phi\rangle_{\text{control}} |\psi\rangle_{\text{target}}$$

The circuit symbols of the CNOT Gate and SWAP Gate are shown below.

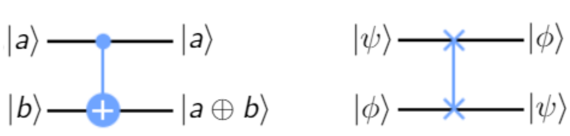


Fig. 2: 2-Qubit Quantum Gates. (Left) Controlled-NOT (CNOT) Gate. $|a\rangle$ and $|b\rangle$ are the control and target qubits respectively. Here, $a, b \in \{0, 1\}$ (Right) SWAP Gate.

The Hadamard Gate, Phase-Shift Gate, Pauli Gates and the CNOT Gate form a *Universal* Gate Set using which any Quantum Circuit may be constructed.

C. Measurement and Conventions

Finally, after completing a Quantum Computation task, a qubit may be measured out in the computational basis. This causes the state of the qubit to collapse to one of the basis states $|0\rangle$ or $|1\rangle$. The value obtained may be stored in a classical register so that they may be used for further processing.

Conventions of Quantum-Computing dictate that all qubits must start out in the state $|0\rangle$ and can only be measured in the computational basis. Other states have to be prepared by applying necessary Unitary Operations, and, measurement in other bases may be performed by using suitable gates before the measurement operation [25].

A quantum circuit for preparing the Bell-State $|\Phi^+\rangle$ and measuring it in the computational-basis illustrates all the operations outlined in this section. (Fig. 3)

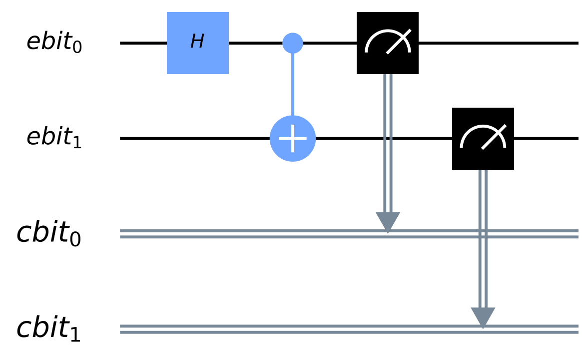


Fig. 3: Quantum Circuit for preparing the Bell-State $|\Phi^+\rangle$, measuring it, and storing the values in a Classical Register.

III. Quantum Communication

The main role of quantum communication is to transmit quantum signals (i.e, quantum states) over large distances from a party Alice to a distant party Bob [1], [2]. Ideally, Alice's state $|\psi\rangle_A$ should be transferred to Bob without any change in its contents. So, the ideal quantum channel (for a 1-qubit state) could be described by the identity map

$$I^{A\to B} = |0\rangle_B \langle 0|_A + |1\rangle_B \langle 1|_A$$

so that, $I^{A\to B} |\psi\rangle_A = |\psi\rangle_B$. Hence, one might suppose that the goal of performing quantum communication is to give Alice and Bob a device to work as the identity map $I^{A\to B}$ [8]. However, interestingly, this is not the only solution. In particular, quantum communication is also possible if the distant parties, Alice and Bob, share an entangled Bell state $|\Phi^+\rangle_{AB}$. In this section, we illustrate this approach through providing representative quantum communication operations, i.e., Quantum Teleportation [3], Superdense Coding [6], and Quantum Key Distribution [1], [30]. As a result, the Bell state is regarded as a resource for quantum communication. [8]

A. Quantum Teleportation

Quantum teleportation [3] is an important primitive of quantum communication operations. If Alice and Bob share an entangled Bell-state between them, then, by using local quantum operations on their respective qubits and classical communication, Alice can transmit any 1-qubit state to Bob. This scheme is known as LOCC (Local Operation + Classical Communication) [31].

The scheme begins with Alice and Bob having access to the corresponding qubits of a Bell-State $|\Phi\rangle_{AB}$. Alice has another qubit in the state -

$$|\psi\rangle_{A'} = \alpha\,|0\rangle_{A'} + \beta\,|1\rangle_{A'}$$

Then, the state of the combined system $A'AB$ is

$$\begin{aligned}|S\rangle_{A'AB} &= |\psi\rangle_{A'} \otimes |\Phi\rangle_{AB} \\ &= \frac{1}{2}\,|\Phi^+\rangle_{A'A} \otimes |\psi_1\rangle_B + \frac{1}{2}\,|\Phi^-\rangle_{A'A} \otimes |\psi_2\rangle_B \\ &+ \frac{1}{2}\,|\Psi^+\rangle_{A'A} \otimes |\psi_3\rangle_B + \frac{1}{2}\,|\Psi^-\rangle_{A'A} \otimes |\psi_4\rangle_B\end{aligned}$$

where, $|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, $|\psi_2\rangle = \alpha\,|0\rangle - \beta\,|1\rangle$, $|\psi_3\rangle = \alpha\,|1\rangle + \beta\,|0\rangle$, $|\psi_4\rangle = \alpha\,|1\rangle - \beta\,|0\rangle$. We can see that the state $|\psi_1\rangle$ is the same as the original state $|\psi\rangle$. So, if Alice performs a Bell-Basis measurement on her qubits A' and A, and, gets the result $|\Phi^+\rangle$, then, we can be sure that the state $|\psi\rangle$ has been transferred to Bob unchanged.

But, the result of of Alice's measurement may also be $|\Phi^-\rangle$, $|\Psi^+\rangle$ or $|\Psi^-\rangle$, in which case the state of Bob's qubit will be $|\psi_2\rangle$, $|\psi_3\rangle$ and $|\psi_4\rangle$ respectively. These states are different from the original state $|\psi\rangle$. But, upon closer observation, we can see that $|\psi_2\rangle$ differs from $|\psi\rangle$ by a phase-flip, $|\psi_3\rangle$ by a bit-flip and $|\psi_4\rangle$ by both a phase-flip and a bit-flip. Hence, if Alice communicates the result of her measurement to Bob (which requires only classical communication) Bob can perform the corresponding correction operation - I (nothing), Z (phase-flip), X (bit-flip), or ZX (phase-and-bit-flip) - on his qubit, and, he will have Alice's original state $|\psi\rangle$ at his disposal. Thus, Alice can transfer the state of her qubit A' just by using the Bell-State $|\Phi^+\rangle$ and classical communication [29].

Since quantum teleportation requires classical communication from Alice to Bob, Bob's system B should work as a quantum memory to keep the quantum state until at least the end of the classical communication. This is important as it inherently implies that quantum teleportation requires the use of a quantum memory [8].

B. Superdense Coding

The mathematical formalism of Superdense Coding [6] is similar to that of the Teleportation Protocol. In this, we use the fact that, any local operation by Alice on her qubit of the shared Bell-Pair $|\Phi^+\rangle_{AB}$ from the set $\{I_A, Z_A, X_A, Z_AX_A\}$ can change the state of the total Bell-Pair system to the states $\{|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}\}$. Now, if Alice sends her part of the Bell-Pair to Bob via a quantum channel, and, Bob performs a Bell-basis measurement on both the qubits, he can find out which operation Alice performed. Since, there are 4 different operations, Alice has transferred the equivalent of 2 bits of information by transmitting a single qubit. This has remarkable possibilities for high-rate data-communication, since, the Bell-pairs may be shared beforehand, and, the channel-bandwidth will be utilized only during the actual time of communication.

C. Quantum Key Distribution

Suppose Alice and Bob possess qubits A and B of the 2-qubit system AB in the Bell-State $|\Phi^+\rangle_{AB}$, and they measure each of their qubits in the computational basis. The Bell state, being a pure state, is not entangled with any other qubits. So, the measurement result does not leave any trace on any other part of the environment from which they can be predicted. As a result, their bits are perfectly secure. In addition, from the definition of the Bell state $|\Phi^+\rangle_{AB} = (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$, the computational basis measurement outcomes always result in both 0's or both 1's, with each occurring randomly 50% of the time. Hence, invoking the one-time pad protocol, Alice and Bob can share a secret bit using the qubits A and B in an information-theoretically secure manner [4], [30]. Therefore, the Bell-Pair can be considered as a cryptographic resource.

IV. Quantum Repeater

The quantum communication tasks outlined in the previous section must start with the distribution of entangled Bell-Pairs between 2 parties. This may be achieved by distributing entangled photons via traditional broadband optical fiber communication links. But, the fidelity of entanglement decreases with the length (L) of the fiber exponentially as e^{-L/L_0}, where L_0 is the attenuation-length of the channel. This necessitates the use of quantum repeaters to allow long-distance communication with finite resources and reasonable rates. In a Quantum Repeater, three primary operations are required to create long-range Bell states. [8] These are:

1) Entanglement Distribution: Creating entangled links between network nodes through the direct transfer of photons.
2) Entanglement Purification: Creating a high-fidelity entangled state from several low-quality ones.
3) Entanglement Swapping: Connecting the entangled links of adjacent nodes using Bell-basis measurement to create long-range entanglement.

Since, direct transfer of photons need to be done only between adjacent repeater nodes, not across the entire long-range link, success probability for generating the entangled link depends only on the distance of the adjacent nodes. This can be reduced arbitrarily as required, by dividing the long-range link into many segments.

A. Quantum Purification

A significant problem of the Bell states generated from an entanglement distribution scheme between the two remote nodes is that they are not perfect. While losses can be mitigated by repeating the scheme many times, other errors will occur in such systems. If the entangled states are stored in matter qubits of a Quantum Memory, they become highly prone to dephasing, i.e, the relative phase between the qubits changes spontaneously. Furthermore, there may be imperfections in the hardware used for state-preparation and measurement. These errors cannot generally be overcome by repetition, and thus, decrease the fidelity of the entangled link.

The fidelity F of a system with density matrix ρ as to how close it is to a state with density matrix σ is defined as,

$$F(\rho,\sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$$

Since, we are comparing the fidelity of our link to the state $|\Phi^+\rangle$, if a dephasing error occurs with probability $1-F$, then our resulting state is given by

$$\rho = F\left|\Phi^+\middle\rangle\middle\langle\Phi^+\right| + (1-F)\left|\Phi^-\middle\rangle\middle\langle\Phi^-\right|$$

where F serves also as the fidelity of the resulting state. Other types of errors associated with imperfect local operations will further decrease this fidelity, inducing errors corresponding to the other three Bell-state elements. This is likely to lead to a maximally mixed state of the form

$$\rho_w = F\left|\Phi^+\middle\rangle\middle\langle\Phi^+\right| + \frac{1-F}{3}\left(\left|\Phi^-\middle\rangle\middle\langle\Phi^-\right| + \left|\Psi^-\middle\rangle\middle\langle\Psi^+\right| + \left|\Psi^-\middle\rangle\middle\langle\Psi^-\right|\right)$$

which is known as the Werner state [32].

1) Bennett's Protocol: The decrease in the quality of entanglement means information present in the state has been lost. In general, it is not possible to recover quantum information without measurement, and thus, destroying the state in the process. However, since we are trying to generate a state that is known beforehand, we can distill a Bell state with higher fidelity from multiple imperfect copies of it by a process known as Quantum Purification [13], [33], [34]. The original purification scheme was proposed by Bennett et al. [13] and is depicted in Fig. 4. It assumes that two copies of the Bell-state have already been established between repeater nodes (which may be of low fidelity). At each node, both the parties apply a CNOT operation between the two qubits keeping the corresponding qubits of each pair as control and target respectively. The target qubits are then measured out in the computational basis $\{|0\rangle, |1\rangle\}$. Finally, the measurement results are transmitted over a classical channel between the nodes.

The resulting state is only kept if the measurement results agree (e.g., $(0,0)$ or $(1,1)$). In such a case the purification is successful. The resulting state of the unmeasured qubit will be of a higher fidelity so long as the initial fidelity of both the pairs were greater than 50% and our local operations (CNOT and the projective measurement) are accurate enough. If the measurement results are not the same (e.g., $(0,1)$ or $(1,0)$), the purification protocol has failed and one needs to start over again with fresh entangled states. This makes the purification protocol inherently probabilistic in nature, but it is heralded. Each party knows whether or not it was successful, but, only after the classical measurement results have been exchanged between the nodes. This is likely to be a significant performance bottleneck.

After a round of purification is performed, the higher-fidelity states may be used again to increase the fidelity even further. In this scheme, quantum purification can be done using a 'Recurrence Method' [13]. However, if the purification fails during any step, the entire process must be started again from new pairs.

This protocol can also be applied if the fidelity of the two Bell-Pairs are not equal [12], [35], in which case the fidelity of the resulting state will be more than that of both the starting states. But, this does result in a relatively lower increase of fidelity per round than the case with equal fidelity states. Schemes which use pairs of unequal fidelity are also called 'Entanglement Pumping' [12].

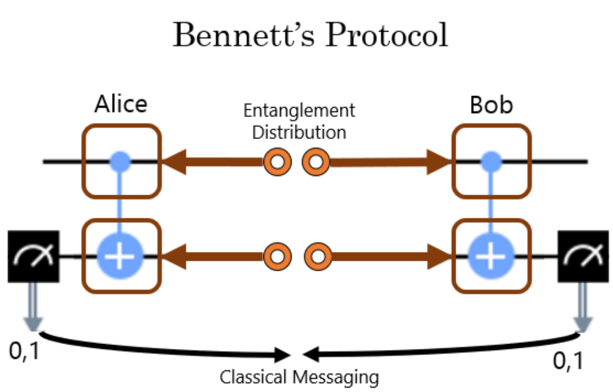


Fig. 4: Schematic illustration of an entanglement purification scheme using two imperfect Bell pairs and local operations including CNOT gates and projective measurements.

2) Deutsch's Protocol: Bennett's protocol suffers from 2 major drawbacks. For it to work, the initial state must be of the Werner form. Secondly, it takes many rounds of purification to obtain a Werner state with fidelity above 99% when one starts with low fidelity pairs (e.g., F = 85%). Deutsch et al. [36] addressed these issues by modifying Bennett's protocol.

The state of a two-level quantum system may be represented as a unit-vector in a 3-dimensional space. This is called the Bloch Vector of the state, and, the sphere on which it resides is called the Bloch Sphere. The unitary operation $R_x(\theta)$ represents rotating the Bloch Vector w.r.t. the x-axis by an angle θ. In matrix notation, it is expressed as,

$$R_x(\theta) = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

Deutsch et al. proposed that, before applying the CNOT Gate, Alice should perform a rotation $R_x(\pi/2)$ on her qubits, and, Bob should perform the inverse rotation $R_x(-\pi/2)$. All the other operations may be performed as in Benett's Algorithm. This procedure results in a theoretical increase in fidelity of about 100 times more than that of Bennett's. Moreover, the initial states of the Bell-Pairs need not be of the Werner form.

3) Multi-Qubit Entanglement Purification: In fact, Deutsch's Protocol can be further generalized. Instead of

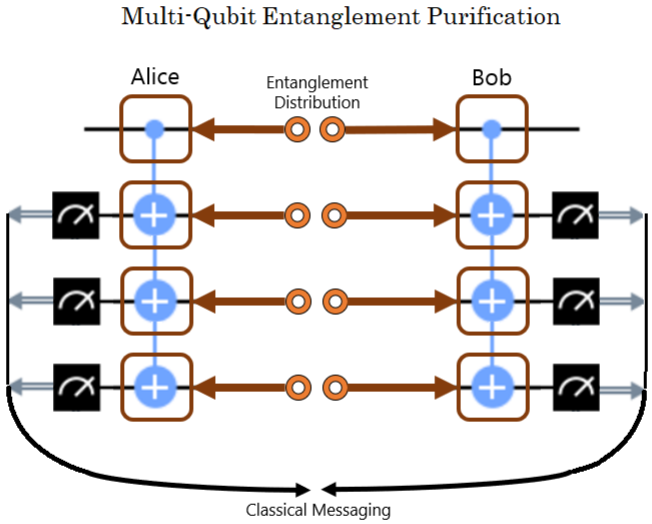


Fig. 5: Schematic illustration of a generalised entanglement purification scheme using n imperfect Bell pairs, local operations and classical communication.

running the purification algorithm on 2 pairs, we can apply it on multiple pairs at the same time [33], [37]. For instance, in the absence of measurement and gate-errors, the 5-qubit variant can theoretically purify 5 imperfect pairs with a fidelity of 0.85 into one with a fidelity above 99% in a single round with a success probability of 0.44 [8]. Significantly more resources and communication time are required if one uses the recurrence method or entanglement pumping (see Fig. 4). A schematic for extending the purification protocol to multiple qubits is given in Fig. 5.

B. Entanglement Swapping

Using entanglement distribution followed by quantum purification, we have a mechanism generate a high-fidelity Bell-State between adjacent repeater nodes. Now, we need a mechanism to connect the individual links together to form a long-range entangled link. This can be achieved with a protocol known as Entanglement Swapping [3], [12].

Consider that we have two Bell-Pairs in the combined state $|\Phi^+\rangle_{12} \otimes |\Phi^+\rangle_{34}$, where the labels 1, 2, 3, 4 indicate the locations of the qubits - of which nodes $(1, 2)$, $(2, 3)$ and $(3, 4)$ are adjacent (Fig. 11). Performing a Bell-state measurement between qubits 2 and 3 projects qubits 1 and 4 into the state $|\Phi^+\rangle_{14}$ up to a Pauli correction operation $\{I, Z, X, Y\}$ depending on the measurement result. The result of the measurement needs to be sent to qubit 4 (or qubit 1 but not both) so that the correction operation can be performed. This is essentially equivalent to the Teleportation protocol, but, the qubit whose state is to be transferred is entangled with another qubit.

The previous discussion assumed ideal Bell states and error-free operations. However because of channel noise and imperfection of local devices, we will instead have mixed states. Modelling these as a Werner state ρ_w with fidelity F, the resulting state after the Bell-state measurement (and correction operations) can be shown also to be a Werner state $\rho_{w_{14}}$ with fidelity $F' = F^2 + (1 - F)^2/3$ [12]. This clearly shows that the fidelity of the longer-range state has decreased compared with the fidelity of the two initial entangled links. In fact, with a good approximation $F' \approx F^2$ for $F \approx 1$. If one is performing entanglement swapping on multiple links (say n links), the resulting fidelity will drop to $F' \approx F^n$. This means purification will need to be performed on longer-range links after carrying out the swapping protocol.

C. Complete Architecture

Now that we have described all the components that go into a Quantum Repeater, we can illustrate how they are put together (see Fig. 7) and how quantum repeaters perform.

Step 1 - First, a number of Bell-Pairs are created between adjacent repeater nodes through entanglement distribution. After generating enough of them, entanglement purification is performed if necessary (either once or a number of times) to increase the fidelity of the link. Two neighbouring high-fidelity links are then connected by using the entanglement swapping protocol to generate a link twice as long as the original one.

Step 2 - Next, quantum purification is performed again on the longer links generated in Step 1. This is again followed by entanglement swapping to create even longer links. In this way, steps 1 and 2 are repeated until an entangled-link of required fidelity is generated between Alice and Bob. If the purification or entanglement swapping fails at any step, we must start over that part again from Step 1. After the entire pipeline of operations is complete, a robust and reliable entangled link will be established between the two parties [12].

The complete architecture of a Quantum Repeater combining all the components mentioned above are illustrated in Fig. 7. Given that the communication link between Alice and Bob

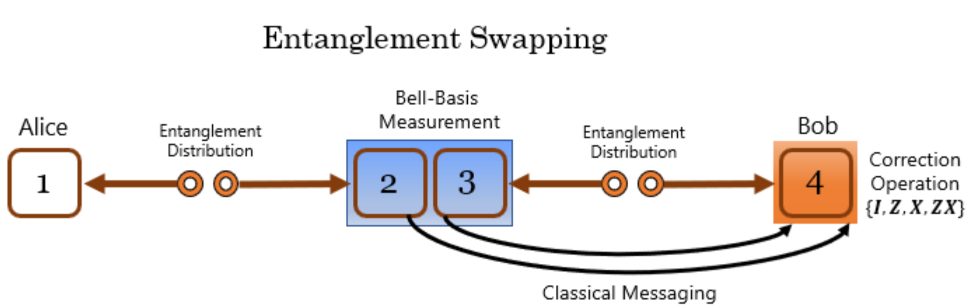


Fig. 6: Schematic of the Entanglement-Swapping Protocol.

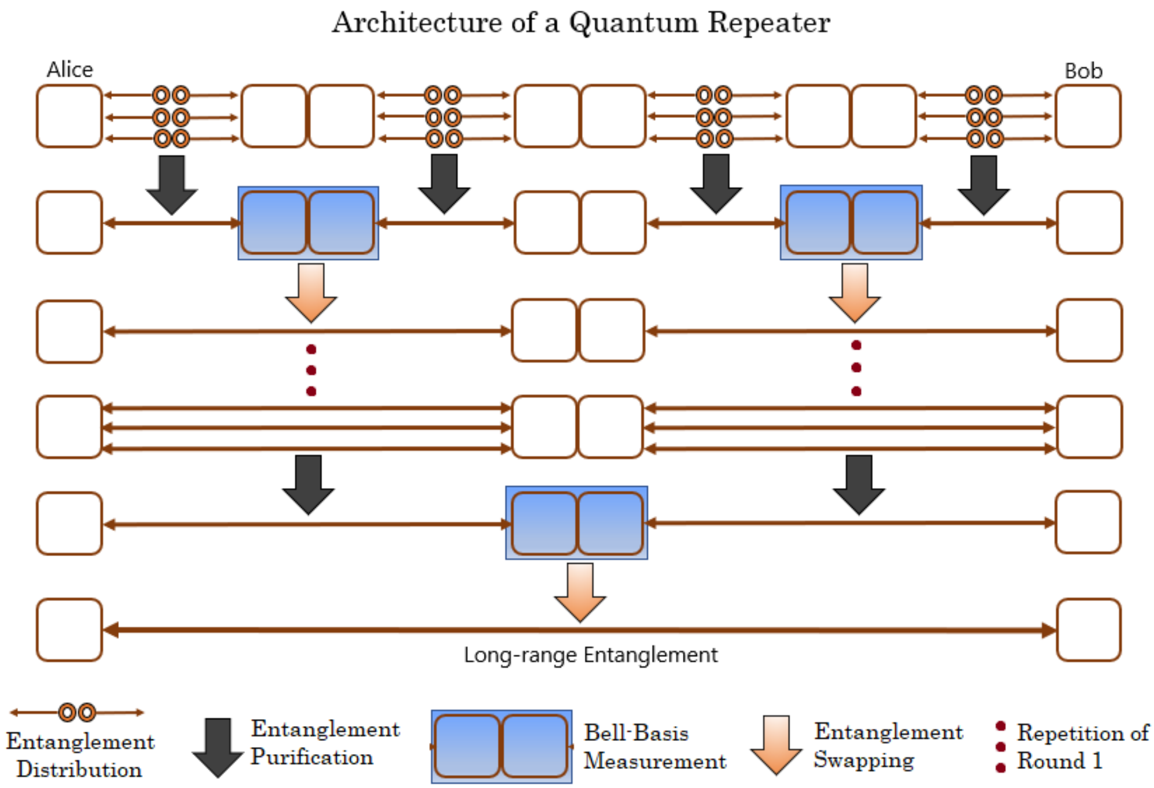


Fig. 7: Quantum repeater scheme for generating long-range entanglement. It begins by splitting the network into a number of segments and placing repeater stations at these nodes. Multiple entangled pairs are then generated between adjacent nodes. These links are then purified and entanglement swapping is performed to create a link twice as long as the original one. These new links are then purified and entanglement swapping is performed again to create a link four times as long. This continues until entanglement is generated between the end repeater nodes (Alice and Bob).

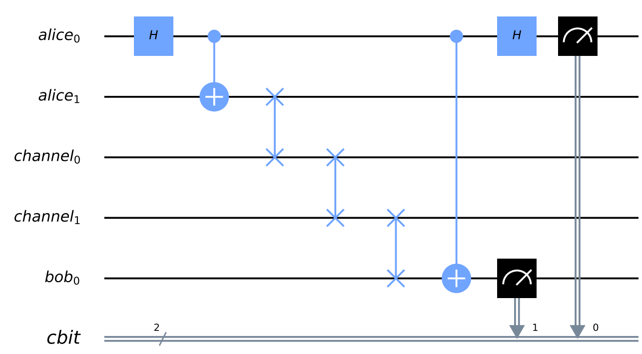
is divided into n segments, a Quantum Repeater can establish long-range entanglement between them after at least $\lceil \log_2 n \rceil$ number of rounds.

V. Experiments and Results

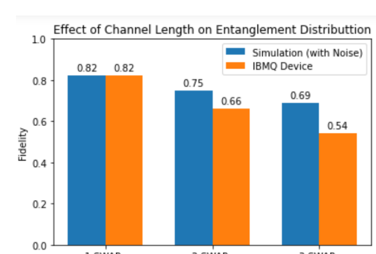
All of the quantum circuits in the experiments were designed using IBM's open-source SDK – Quantum Information Science toolKit (QISKit) in Python. The circuits were run on IBMQ-16-Melbourne - a real quantum computing device with 15 superconducting qubits, through backend-access via the cloud. After performing the experiments, they were error-corrected using QISKit's Ignis library and its Error-Mitigation protocols to remove the effects of measurement-errors in the results. In addition, the circuits were also simulated natively using QISKit's 'QASM Simulator' with a noise model from QISKit's Aer library that mimics the device-noise of IBMQ-16-Melbourne. The simulation results provide a reference point to which the device results can be compared.

A. Channel-Length Simulation

First, the effect of channel-length on entanglement distribution was examined. The circuit used for this is shown in Fig. 8. Here, transmitting a qubit directly to a quantum channel is emulated by using the SWAP gate. The number of SWAP gates applied emulates the length of the channel. The effect



(a) label 1



(b) label 2

Fig. 8: 2 Figures side by side

of the number of SWAP gates on the fidelity of entanglement is shown in Fig. 8.

It is worth noting, just after 3 SWAP Gates, the fidelity of the Bell-pair falls below 50% making it unusable for further processing. This is representative of the number of consecutive operations that can be performed faithfully on current quantum computers.

B. Quantum Purification

The quantum circuit for performing Bennett's Quantum Purification Protocol with Deutsch's correction operations on 3 Bell-pairs is shown in Fig. 9. The results of executing this circuit on IBMQ are shown in Fig. 10. They show the effect of the number of qubits used in one round of purification on the the yield and fidelity of entanglement. We define the yield to be the percentage of times in which the classical messages between Alice and Bob agree, and, the protocol is successful. Since, agreement of classical messages is heralded, the fidelity of entanglement is calculated only when the protocol is successful.

Although the 3-qubit protocol should theoretically perform better than the 2-qubit one, the results show otherwise. This is due to the fact that, a higher number of gate-operations are required to run purification on 3 qubits simultaneously. Since the gate operations are imperfect, this induces a greater amount of noise in the system nullifying any theoretical advantage.

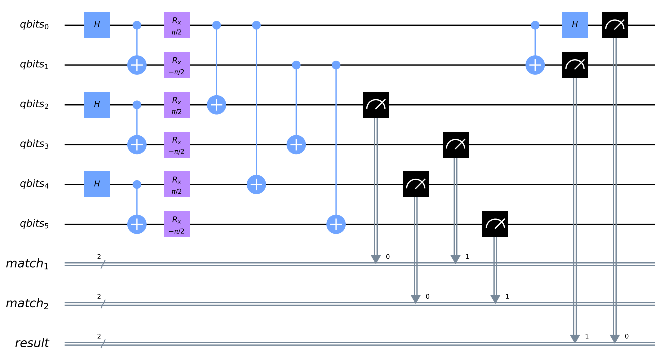
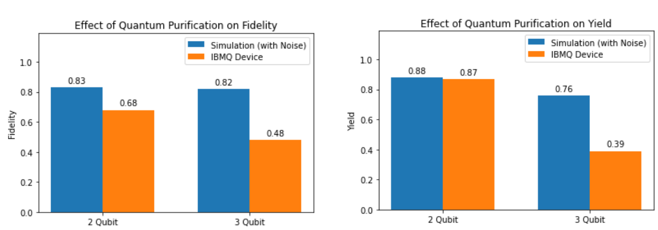


Fig. 9: Quantum Circuit for implementing a 3-Qubit extension of Deutsch's Protocol.



(a) Fidelity (b) Yield

Fig. 10: Effect of Deutsch's Quantum Purification Protocol on (a) Fidelity of Quantum Entanglement and (b) Yield of Entangled Qubits

C. Entanglement Swapping

Next, Fig. 11 shows quantum circuit for performing the Entanglement Swapping protocol with one repeater node in the middle. The results of running this circuit on IBMQ is shown in Fig. 12. As can be seen, entanglement swapping causes a large loss in the fidelity of entanglement. This necessitates further purification of the swapped qubits.

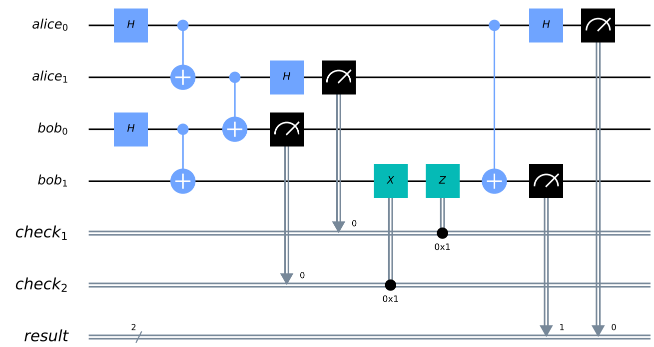


Fig. 11: Quantum Circuit of the Entanglement-Swapping Protocol.

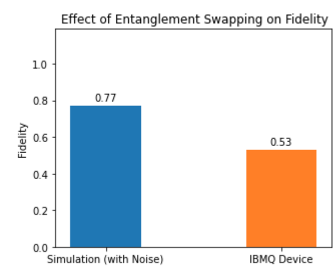


Fig. 12: Results of testing the Entanglement Swapping Protocol.

D. Quantum Repeater

Finally, the full quantum circuit of a Qauntum Repeater integrating all the elements discussed above is shown in Fig. 13.

In it, Alice and Bob first prepare 3 Bell-pairs. Alice transfers one qubit from each of her pairs to the channel (emulated by using SWAP gates). Then, entanglement-swapping takes place between the channel-qubits and Bob's qubits. After that, Alice and Bob use the R_x gate on their qubits according to Deutsch's Protocol, and, use the CNOT operations according to Bennett's Protocol. 2 qubits each of Alice and Bob are measured out and communicated to each other to check if the Entanglement Purification was successful. Finally, The remaining qubits of Alice and Bob are measured out in the Bell-basis to check the fidelity of entanglement established between them.

The results of running the circuit, on the final fidelity of entangled qubits and their yield, are shown in Fig. 14. These demonstrate how the repeater protocol performs under hardware imperfections to establish long-range entanglement between two qubits in existing hardware.

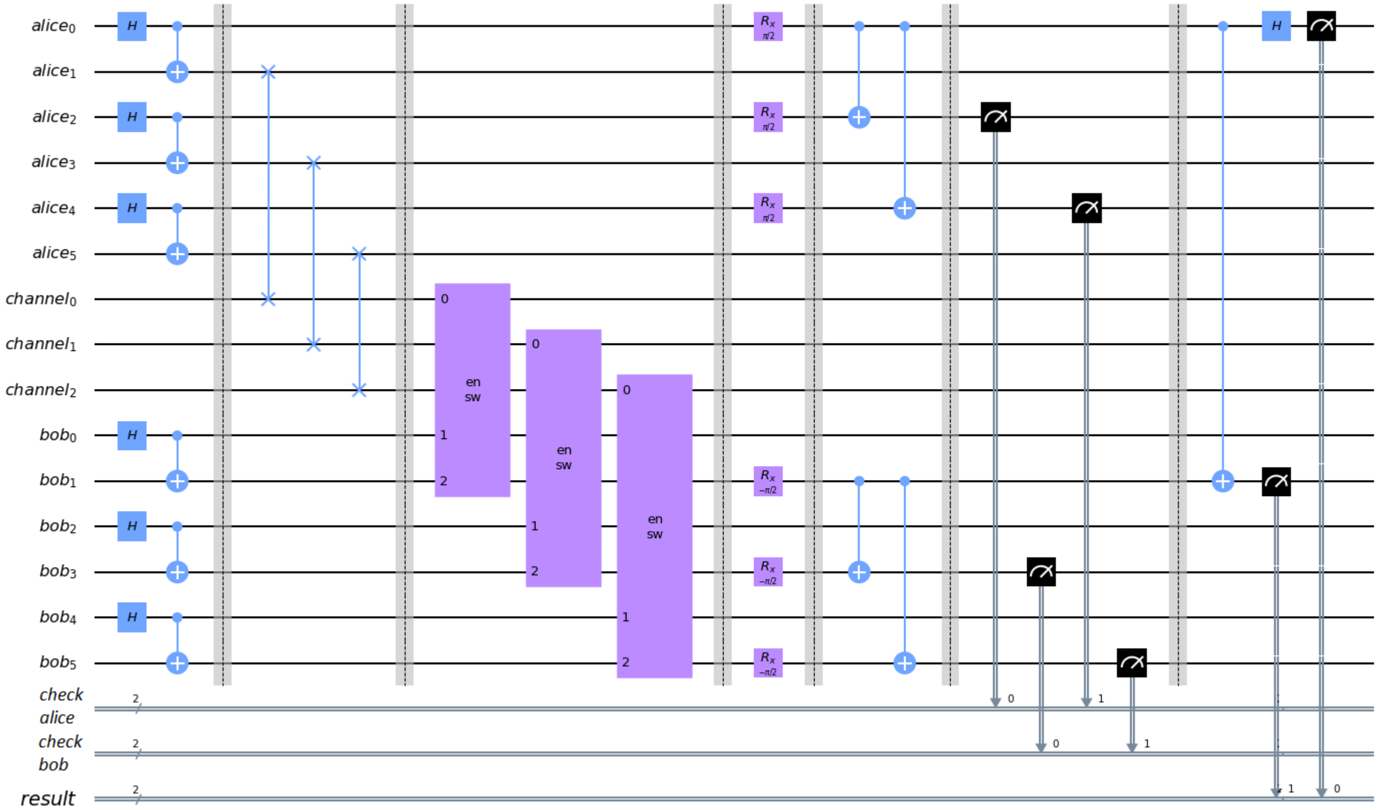
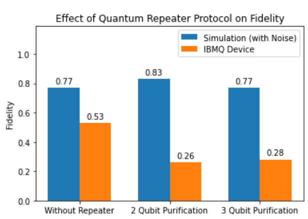
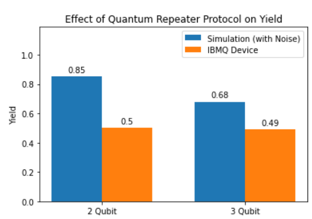


Fig. 13: Complete circuit of the proposed Quantum Repeater Architecture.



(a) Fidelity



(b) Yield

Fig. 14: Performance of the Quantum Repeater Circuit on (a) Fidelity of Quantum Entanglement and (b) Yield of Entangled Qubits

VI. Discussion

In this paper, we have demonstrated the complete circuit-level implementation of a Quantum Repeater, and, its performance on IBM's cloud Quantum Computer. The experiments demonstrate the efficacy of the different elements of a Quantum Repeater in increasing the fidelity of distributed Bell-Pairs and establishing long-range links. It is interesting to note that, although theoretical calculations and simulation results indicate an increase in fidelity from using a quantum repeater instead of direct transmission, the results from IBMQ indicate less stellar performance at present. To construct a full-fledged quantum repeater, a multitude of operations need to be performed on entangled qubits while protecting their coherence at the same time. But, as the number of operations increase, gate-errors, measurement-errors and dephasing become insurmountable, making the qubits unsuitable to work with. Thus, the results reveal the current state of IBM's Quantum hardware, as to the number of quantum operations that can be done before the errors become unmitigable. Due to this constraint, complex purification protocols with large number of operations cannot be emulated as of now.

There is much scope to extend this work even further. A promising direction is to come up with robust and condense Error-Correcting Codes, so that, the fidelity may be increased without discarding all the Bell-pairs. This will result in higher yield-rates without sacrificing the error-rates. Another approach would be to co-design hardware-specific error-correcting codes, taking into account the device-architecture of a quantum system, so that errors can be mitigated more efficiently. The present work can be a useful guide in that direction.

Acknowledgment

Sowmitra Das would like to thank Md. Shahnewaz Ahmed of the Dept. of CSE, BRAC University for helping him gain insight into the nature of entanglement and its role in Quantum Communication. His advice, comments and guidance were vital in making the experiments a reality.

References

[1] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Conf. on Computers, Systems and Signal Processing (Bangalore, India*, 1984, pp. 175–9.

[2] N. Gisin and R. Thew, "Quantum communication," *Nature photonics*, vol. 1, no. 3, pp. 165–171, 2007.
[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bellâs theorem," *Physical review letters*, vol. 68, no. 5, p. 557, 1992.
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.
[6] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states," *Physical review letters*, vol. 69, no. 20, p. 2881, 1992.
[7] S. Van Enk, J. Cirac, and P. Zoller, "Photonic channels for quantum communication," *Science*, vol. 279, no. 5348, pp. 205–208, 1998.
[8] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside Quantum Repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 78–90, May 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7010905/
[9] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
[10] D. Dieks, "Communication by epr devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.
[11] J. L. Park, "The concept of transition in quantum mechanics," *Foundations of Physics*, vol. 1, no. 1, pp. 23–33, 1970.
[12] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.
[13] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical review letters*, vol. 76, no. 5, p. 722, 1996.
[14] Q. Ruihong and M. Ying, "Research progress of quantum repeaters," *Journal of Physics: Conference Series*, vol. 1237, p. 052032, jun 2019. [Online]. Available: https://doi.org/10.1088%2F1742-6596%2F1237%2F5%2F052032
[15] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li *et al.*, "Experimental quantum repeater without quantum memory," *Nature Photonics*, vol. 13, no. 9, pp. 644–648, 2019.
[16] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, "Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission," *Physical Review A*, vol. 99, no. 5, p. 052330, 2019.
[17] J. Borregaard, H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen, "One-way quantum repeater based on near-deterministic photon-emitter interfaces," *Physical Review X*, vol. 10, no. 2, p. 021071, 2020.
[18] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018. [Online]. Available: https://doi.org/10.22331/q-2018-08-06-79
[19] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys*, vol. 21, no. 6/7, 1982.
[20] A. Cross, "The ibm q experience and qiskit open-source quantum computing software," *APS*, vol. 2018, pp. L58–003, 2018.
[21] G. Aleksandrowicz *et al.*, "Qiskit: An Open-source Framework for Quantum Computing," January 2019. [Online]. Available: https://doi.org/10.5281/zenodo.2562111
[22] B. K. Behera, S. Seth, A. Das, and P. K. Panigrahi, "Demonstration of entanglement purification and swapping protocol to design quantum repeater in ibm quantum computer," *Quantum Information Processing*, vol. 18, no. 4, p. 108, 2019.
[23] A. Zhukov, E. Kiktenko, A. Elistratov, W. Pogosov, and Y. E. Lozovik, "Quantum communication protocols as a benchmark for programmable quantum computers," *Quantum Information Processing*, vol. 18, no. 1, p. 31, 2019.
[24] D. E. Deutsch, "Quantum computational networks," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 425, no. 1868, pp. 73–90, 1989.
[25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
[26] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical review A*, vol. 52, no. 5, p. 3457, 1995.
[27] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.
[28] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, p. 777, 1935.
[29] B. Schumacher and M. Westmoreland, *Quantum processes systems, and information*. Cambridge University Press, 2010.
[30] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.
[31] A. Peres and W. K. Wootters, "Optimal detection of quantum information," *Physical Review Letters*, vol. 66, no. 9, p. 1119, 1991.
[32] R. F. Werner, "Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model," *Physical Review A*, vol. 40, no. 8, p. 4277, 1989.
[33] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, p. 3824, 1996.
[34] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Physical Review A*, vol. 79, no. 3, p. 032325, 2009.
[35] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, "System design for a long-line quantum repeater," *IEEE/ACM Transactions on Networking*, vol. 17, no. 3, pp. 1002–1013, 2008.
[36] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Phys. Rev. Lett.*, vol. 77, pp. 2818–2821, Sep 1996. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.77.2818
[37] H. Aschauer, "Quantum communication in noisy environments," Ph.D. dissertation, lmu, 2005.