ENHANCED ARCHITECTURE FOR ASYMMETRIC QUANTUM SYNDROME ERROR CORRECTION

Thesis

Submitted in partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

MUMMADI SWATHI

(Reg. No.: 197064IT001)

DEPARTMENT OF INFORMATION TECHNOLOGY
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575025

MAY, 2023

Declaration

I hereby *declare* that the Research Thesis entitled **"Enhanced Architecture for Asymmetric Quantum Syndrome Error Correction"** which is being submitted to the **National Institute of Technology Karnataka, Surathkal** in partial fulfilment of the requirements for the award of the Degree of **Doctor of Philosophy** in **Information Technology** is a *bonafide report of the research work carried out by me.* The material contained in this thesis has not been submitted to any University or Institution for the award of any degree.

01|6|23

Mummadi Swathi
Reg.No. 197064IT001
Department of Information Technology
NITK, Surathkal, India

Place : NITK, Surathkal
Date : 01-06-2023

Certificate

This is to *certify* that the Research Thesis entitled **"Enhanced Architecture for Asymmetric Quantum Syndrome Error Correction"** submitted by **Mummadi Swathi (Registration Number: 197064IT001)** as the record of the research work carried out by her, is *accepted as the Research Thesis submission* in partial fulfilment of the requirements for the award of degree of Doctor of Philosophy.

Place : NITK, Surathkal
Date : 01 - 06 - 2023

01/06/2023
Dr. Bhawana Rudra
Research Guide
Assistant Professor
Department of Information Technology
NITK Surathkal - 575025

02/06/2023
Chairman - DRPC
(Signature with Date and Seal)

CHAIRMAN - DRPC
Department of Information Technology
NITK Surathkal, Srinivasnagar P.O.
Mangaluru 575 025, INDIA

Dedicated to

My Husband & Son

Acknowledgements

First and foremost, I would like to thank from the bottom of my heart my beloved guide **Dr. Bhawana Rudra**, Assistant Professor, Department of Information Technology, NITK Surathkal for her eminent guidance, continuous inspiration and unconditional support that I received throughout the course of my research. This research would have not possible without her support and timely inputs.

I would also like to extend my gratitude to my RPAC panel, **Prof. G. Ram Mohana Reddy**, Department of Information Technology and **Dr. Prabhu K**, Department of Electronics and Communication Engineering for their valuable feedback and constructive suggestions during my research work.

Special thanks to my husband **U. Gnaneshwara Chary** for his love, patience and unconditional support during my research work. I also thank my lovely son **U. Bruhadh Vashishta Chary** for his unconditional cooperation. Without their support, I would have not completed my research work. I also thank my parents and in-laws for their blessings. I also thank all my family members for their support.

I would like to thank all my lab mates and fellow research scholars for the many productive discussions and fun moments that will be in my memories forever. Finally I would like to thank all the teaching, technical, administrative, as well as non-teaching staff of the Department of Information Technology, who have been very kind and helpful throughout my research work. My heartfelt gratitude to **NITK Surathkal** for making this research memorable and possible.

(Mummadi Swathi)

Abstract

Quantum computing is a new edge technology developed over the principles of Quantum Physics and mechanics. As these systems compute exponentially faster than classical systems, researchers started to implement their applications in numerous domains such as security, communication, networking etc. The fundamental unit of measuring information in quantum systems is Quantum bits or qubits generated from the electron/proton particles. As per the behaviour of a photon particle, it leads to noise whenever the operations are performed with these particles. The currently developed quantum systems are in the Noisy Intermediate Scale Quantum (NISQ) Level. The error rate in NISQ systems is exorbitant due to operational noise and decoherence. Thus, developing an efficient Quantum Error Correction mechanism is inevitable to protect the information from errors. As most of the existing QEC methods are symmetric, they are implemented by assuming the probability of getting phase and bit flip errors as the same. However, due to the fragility of the quantum particles, the possibility of getting phase flip errors is more than the bit flip errors. Hence, the concept of Asymmetric Quantum Error Correction has been introduced as a solution. In current scenario, there is a lot of scope for significant improvements in Asymmetric Quantum Error Correction in terms of Fidelity, Quantum depth, Quantum cost, and Number of Qubits used to perform error detection and correction efficiently. It has been observed from the literature that the entangled qubits play a significant role in Asymmetric Quantum Error Correction to detect and correct the errors.

This thesis presents a novel and efficient Asymmetric Quantum Error Correction method with Syndrome Measurement. In order to improve the efficiency of error correction, entangled qubits are used along with the original quantum information. Whenever entangled qubits are used to perform any operation, it is essential to consider the maximally entangled qubits to avoid errors or data loss. To address this challenge, an efficient entanglement swapping-based purification protocol is proposed to distil the maximally entangled qubits from the deficient entangled qubits. In order to quantify the efficacy with respect to the Quantum Cost of the proposed model, an efficient Quantum cost optimization algorithm is proposed with unit cost quantum gates to investigate and optimize the Asymmetric Quantum Error Correction. Finally, the proposed Quantum Error Correction method is used to develop a Quantum key distribution protocol for secure data transmission. From the experimental results, it is observed that the proposed algorithms outperform the existing state-of-the-art methods in terms of Fidelity, Quantum cost, Quantum depth, and Communication efficiency when executed over a real quantum system.

Keywords: Quantum Information; Quantum States; Qubits; Quantum Errors; Entanglement Purification; Asymmetric Quantum Error Correction; Entanglement based Asymmetric Quantum Error Correction; Quantum Cost; Quantum Depth; Quantum Cost Optimization; Quantum Key Distribution.

Contents

List of Figures v

List of Tables ix

List of Abbreviations x

1 Introduction 1

1.1 Fundamentals of Quantum computation 2

1.1.1 Superposition 2

1.1.2 Entanglement 3

1.1.3 Quantum Teleportation 4

1.2 Reversible Operations 5

1.3 Reversible Quantum gates 6

1.3.1 Single qubit gates 6

1.3.2 Multi qubit gates 9

1.4 Quantum Errors 10

1.5 Error Correction mechanism in Quantum Computing 11

1.6 Ancilla Qubits 12

1.7 Motivation 12

1.8 Summary 13

1.9 Organization of the Thesis 14

2 Literature Survey 15

2.1 Quantum Computing and Error Correction 15

2.2 Various approaches in Quantum Error Correction 17

2.2.1 Additive Quantum Error Correction codes 18

2.2.2 Non-additive Quantum codes 24

2.2.3 Entanglement Assisted Quantum codes 25

2.2.4 Asymmetric Quantum codes 26

2.3 Entanglement purification 30

2.4 Quantum Cost Optimization 34

2.5 Quantum Key Distribution 37
2.6 Research gaps 39
2.7 Problem Statement 40
2.8 Objectives 40
2.9 Summary 40

3 Architecture for Asymmetric quantum Syndrome Error Correction 41

3.1 Brief overview of Proposed Methodology 41
3.1.1 Entanglement Purification 41
3.1.2 Asymmetric Quantum Syndrome Error Correction 43
3.1.3 Quantum Cost Optimization 44
3.1.4 Quantum Key Distribution 44
3.2 Research Contributions 45
3.3 Summary 46

4 Entanglement Purification using Entanglement Swapping 47

4.1 Importance of Entanglement Purification 47
4.2 Entanglement Generation 47
4.2.1 Entanglement generation using 2-Qubits (Bell pair $|\phi^+\rangle_{AB}$) 50
4.2.2 Entanglement generation using 4-Qubits (Bell pair $|\phi^+\rangle_{AB}$) 52
4.3 System Probability, Error rate and Fidelity Measurement 54
4.3.1 Probability and Error rate Measurement 54
4.3.2 Fidelity Measurement 55
4.4 Entanglement Swapping 56
4.5 Experimental Setup 60
4.6 Discussion and Result Analysis 61
4.6.1 Discussion 61
4.6.2 Result Analysis 64
4.7 Summary 66

5 Asymmetric Quantum Syndrome Error Correction 69

5.1 Importance of Quantum Error Correction 69
5.2 Quantum Information Process (QIP) with Error Correction Method . 69
5.3 Phase gate(S) and Unitary operations 70
    5.3.1 S gate 70
    5.3.2 Unitary operation 71
5.4 Quantum Channel & Channel Noise 71
    5.4.1 Depolarization noise 71
    5.4.2 Amplitude Damping Noise 72
5.5 Proposed Methodology 72
    5.5.1 Encoding the Quantum Information 73
    5.5.2 Error Detection and Correction 78
    5.5.3 Decoding the Quantum Information 81
5.6 Experimental Setup 83
5.7 Discussion & Result Analysis 84
5.8 Asymmetric Quantum Syndrome Error Detection and Correction using Entangled qubits 86
    5.8.1 Experimental Setup 87
    5.8.2 Result Analysis 89
5.9 Summary 91

6 Quantum Cost Optimization 93

6.1 Importance of Quantum Cost Optimization 93
6.2 Quantum Cost and Unit cost Quantum gates 94
    6.2.1 Quantum cost 94
    6.2.2 Unit cost Quantum Gates 95
6.3 Proposed methodology for Quantum cost optimization 97
    6.3.1 Optimization algorithm for Toffoli gate 99
    6.3.2 Optimization algorithm for Peres gate 101
    6.3.3 Optimization algorithm for Entanglement purification method 102
    6.3.4 Optimization algorithm for Entanglement based Asymmetric Quantum Error Correction 104

6.4 Experimental Setup 107
6.5 Result Analysis and Discussion 108
  6.5.1 Quantum Cost Calculation using RCViewer tool 109
6.6 Summary 110

7 Quantum Key Distribution 113

7.1 Significance of Quantum Error Correction in Quantum key Distribution 113
7.2 Proposed Methodology 115
  7.2.1 Entanglement Generation and Entanglement Purification . . 116
7.3 Experimental setup and Result Analysis 121
  7.3.1 Experimental Setup 121
  7.3.2 Result Analysis 122
  7.3.3 Calculation of QKD communication efficiency 123
7.4 Third party Risk Analysis 125
  7.4.1 Third party detection rate 126
7.5 Summary 127

8 Conclusion and Future Work 129

APPENDIX 133

A Experimental Analysis of a Quantum Encoder in Various Quantum Systems 133

A.1 Proposed Encoder and its implementation in Quantum systems . . . 133
A.2 Result analysis of various Quantum systems 137
A.3 Summary 138

References 141

Publication Details 157

List of Figures

1.1 Bloch Sphere. The arbitrary representation of a Quantum State $|\psi\rangle$ with respect to the X, Y and Z basis 2

1.2 The process of Quantum Teleportation 5

1.3 Graphical representation of SWAP Gate 9

1.4 Graphical representation of CNOT Gate 9

2.1 Steps in Quantum Information Process 16

2.2 Error correction procedure in Additive Codes (Ezerman et al. (2011)). 18

3.1 Architecture for Asymmetric Quantum Syndrome Error Correction . 42

3.2 Workflow of Entanglement Purification 43

3.3 Methodology for Asymmetric Quantum Syndrome Error Correction 43

3.4 Methodology for Quantum Cost Optimization 44

3.5 Process of Quantum Key Distribution 45

4.1 Quantum Circuit diagram for 2-Qubit Entanglement. q_0 and q_1 are input variables and c2 is an output variable. This circuit illustrates the Bell state $|\phi^+\rangle$ with inputs $|0\rangle$ and $|1\rangle$. 50

4.2 Probability Measurement Chart of 2-Qubit Entanglement Circuit after running in the IBM Quantum System. 51

4.3 Transpiled Circuit diagram of 2-Qubit Entanglement. 52

4.4 Quantum Circuit diagram for 4-Qubit Entanglement. Here q_0, q_1, q_2, q_3 represents the inputs and c4 represents the output 52

4.5 Probability Measurement Chart of 4-Qubit Entanglement after running in Quantum system. 53

4.6 Transpiled Circuit diagram of 4-Qubit Entanglement. 53

4.7 Representation of 4-stage Entanglement Swapping with Bell State Measurement (BSM). Here total 4 Entangled Pairs(EP's) and 3-BSM's are used to perform Entanglement Swapping. 56

4.8 Quantum results for 4-Qubit Entanglement generation. 61

4.9 Quantum results for 4-Qubit Entanglement purification after swapping. 62

4.10 Probability comparisons of Figures 4.8, 4.9 63

4.11 Bloch sphere representation of 4-Qubit Entanglement purification with swapping. 63

4.12 Probability measurement of the first and last entangled qubits ($|q_0\rangle$ & $|q_3\rangle$) in Quantum system 64

4.13 Probability measurement of the second and third entangled qubits ($|q_1\rangle$ & $|q_2\rangle$) in Quantum system 64

4.14 Probability measurement of the first and last entangled qubits ($|q_0\rangle$ & $|q_3\rangle$) in Quantum simulator 65

4.15 Probability measurement of the second and third entangled qubits ($|q_1\rangle$ & $|q_2\rangle$) in Quantum simulator 65

4.16 Fidelity Analysis of Existing and Proposed Methods with Quantum System Results. 66

4.17 Fidelity Analysis of Existing and Proposed Methods with Simulator Results. 66

5.1 Quantum Information Process with error correction approach 70

5.2 Asymmetric Quantum Error Correction with Encoding, Syndrome measurement, and Decoding procedure 73

5.3 Quantum results for Encoding Quantum Information 76

5.4 Density matrix of encoding method with all possible states with real and imaginary values Re[ρ], Im[ρ] respectively 77

5.5 Bit and Phase error representations a) Represents the actual state $|\phi\rangle$ and bit flip of state $X|\phi\rangle$ with probabilities P_r and $1 - P_r$ b) Represents the actual state $|\phi\rangle$ and phase flip of state $Z|\phi\rangle$ with probabilities P_r and $1 - P_r$ 77

5.6 Quantum results for Syndrome measurement 81

5.7 Quantum results for Decoding the quantum information 82

5.8 Density matrix of Decoding method with all possible states with real and imaginary values Re[ρ], Im[ρ] respectively 83

5.9 Quantum results for the proposed Asymmetric Quantum Syndrome Error Correction with Encoding, Error Detection & Correction and Decoding steps. 84

5.10 Result Analysis of proposed AQEC with existing methods 86

5.11 The process of Asymmetric Quantum Error Correction (AQEC) using Entanglement 87

5.12 Quantum system result for AQSEC with Entangled qubits. 89

5.13 Quantum Simulator result for AQSEC with Entangled qubits. 90

5.14 Result Analysis of proposed Asymmetric Quantum syndrome Error correction using Entangled Qubits with existing methods 90

6.1 a) Controlled V gate b) Controlled V^+ gate 96

6.2 Procedure for Quantum Cost Optimization 98

6.3 Block diagram of Toffoli gate 99

6.4 Quantum Circuit diagram of Toffoli gate. Here q_0, q_1, q_2 represents the quantum states 100

6.5 State vector diagram of Optimized Toffoli gate algorithm in Quantum system for input combination $|010\rangle$. 100

6.6 Block diagram of Peres gate 101

6.7 Quantum Circuit diagram of Peres gate 101

6.8 State vector diagram of Optimized Peres gate algorithm in Quantum system for input combination $|001\rangle$. 102

6.9 Quantum system Results of Entangled pair [q0,q3] 104

6.10 Quantum system Results of Entangled pair [q1,q2] 104

6.11 Architecture of optimized Entanglement based Quantum Error Correction 105

6.12 Quantum system results for optimized AQSEC using entangled Qubits 107

6.13 Result analysis of optimized Entanglement Purification method with existing works 109

6.14 Result analysis of optimized AQEC with existing QEC models . . . 110

7.1 Process of Quantum key distribution 114

7.2 Quantum key distribution with Entanglement purification and Asymmetric Quantum Error correction 116

7.3 Quantum key distribution results with and without entanglement purification 122

7.4 Result analysis of Quantum key length in Quantum System 123

7.5 Result analysis of Quantum key length in quantum Simulator . . . 124

7.6 Analysis of Error rate 125

7.7 Third party Interference in QKD 126

7.8 Third party risk analysis 126

A1 Encoder results on system ibmq_quito 134

A2 Encoder results on system ibmq_lima 135

A3 Encoder results on system ibmq_belem 135

A4 Encoder results on system ibmq_bogota 135

A5 Encoder results on system ibmq_manila 136

A6 Encoder results on system ibmq_jakarta 136

A7 Encoder results on system ibm_perth 137

A8 Analysis between Number of qubits, Quantum Volume and Program Run time. 138

List of Tables

7.1 Analysis of QKD Communication Efficiency 125

A1 Comparison of results with various quantum systems 138

List of Abbreviations

Abbreviation	Meaning
AQC	Asymmetric Quantum Code
AQCC	Asymmetric Quantum Concatenated Code
AQEC	Asymmetric Quantum Error Correction
AQCTPC	Asymmetric Quantum Concatenated and Tensor Product Code
AQSEC	Asymmetric Quantum Syndrome Error Correction
BCH	Bose–Chaudhuri–Hocquenghem
CC	Concatenated Code
CNOT	Controlled NOT
CPC	Coherent Parity Check
CPCC	Coherent Parity Check Codes
CPF	Controlled Phase Flip
CPHASE	Controlled Phase
CSS	Calderbank-Shor-Stene
CTQEC	Continuous Time Quantum Error Correction
CWS	Code Word Stabilizer
DLP	Data Loss Prevention
DOF	Degrees of Freedom
EACQC	Entanglement Assisted Concatenated Quantum Codes
EAQEC	Entanglement Assisted Quantum Error Correction
ECS	Entangled Coherent States
EPP	Entanglement Purification Protocol
GLLP	Gottesman, Lo, Lütkenhaus and Preskill
GV	Gilbert–Varshamov
LDPC	Low Density Parity Check
LILLIPUT	Lightweight Low-Latency Lookup-Table
LUT	Look Up Table
MBEPP	Measurement Based Entanglement Purification Protocol
MEPP	Multipartite Entanglement Purification Protocol
MES	Maximally Entangled State
MIMO	Multi Input Multi Output
NISQ	Noisy Intermediate Scale Quantum
QBER	Quantum Bit Error Rate
QC	Quasi Cyclic
QEC	Quantum Error Correction

QECC	Quantum Error Correction Code
QIP	Quantum Information Process
QISKIT	Quantum Information Software Kit
QKD	Quantum Key Distribution
QLDGM	Quantum low-density-generator-matrix
QLDPC	Quantum Low Density Parity Check
QMDS	Quantum Maximum Distance Separable
QND	Quantum Non-Demolition Measurements
QSC	Quantum Stabilizer Code
QTECC	Quantum Topological Error Correction Code
RNN	Recurrent Neural Network
RSA	Rivest–Shamir–Adleman
SFG	Sum Frequency Generation
SFQ	Single Flux Quantum
SPDC	Spontaneous Parametric Down Conversion
SQV	Simple Quantum Volume
TPC	Tensor Product Code

Chapter 1

Introduction

Quantum computing is a field of computer science that seeks to exploit the unique properties of quantum systems. It performs computational tasks that are beyond the capabilities of classical computers. Quantum computing was first introduced by Paul Benioff in the early 1980s (Benioff, 1982). He implemented a Turing machine based on quantum mechanical principles. Richard Feynman proved that quantum computers are exponentially powerful compared to classical computers (Feynman, 1985). This experiment was a big breakthrough and motivated many researchers to enact quantum technology in various fields like chemistry, networking, security, communication and more. In 1994, Peter Shor introduced an algorithm named Shor's for integer factorization (Shor, 1995). Shor's algorithm has proved that the RSA algorithm can easily breakable using a quantum computer. Most of the current security systems are implemented based on the RSA algorithm. Due to this, the research in quantum computing has increased. Many companies are working on the development of full-fledged Quantum computers to overcome the issues of classical computers and to solve complex problems in various fields.

Initially, all the quantum experiments were performed either mathematically or theoretically. With the existence of Quantum system, it is possible to perform experiments on real quantum computers. With this, it is also possible to observe how the quantum particle reacts to the various operations. Quantum particles are generated from the photon/electron sources and are prone to errors due to noise. The noise is generated when quantum particles interact with the external environment to perform the operations. Thus, the currently available quantum systems are in the Noisy Intermediate Scale Quantum (NISQ) level with a high error rate (Singh Gill et al., 2020). With this, the importance of error correction methods in quantum computing has been increased. To be precise, we cannot imagine a quantum system without an error correction mechanism. Before discussing about quantum error correction, it is necessary to know about the basics of quantum computation like superposition, entanglement, etc., and various quantum gates which are required in chapter 4, 5, 6, 7. A detailed discussion on these topics is given in section 1.1.

1.1 Fundamentals of Quantum computation

In classical computing, the information is measured in terms of binary bits 0 and 1. These can be in any one of the states at a time. In quantum computing, the information is measured in terms of qubits where qubit is a superposition of quantum states $|0\rangle$ and $|1\rangle$. A qubit can be in both states at a time (De Ronde, 2018). Thus it can perform 2^n operations at a time with n qubits, whereas in classical computation we can perform only one operation at a time. The property of superposition made quantum computers exponentially powerful compared to classical computation.

1.1.1 Superposition

A qubit's superposition is graphically represented using the Bloch sphere (Bloch, 1946) as shown in Figure 1.1.

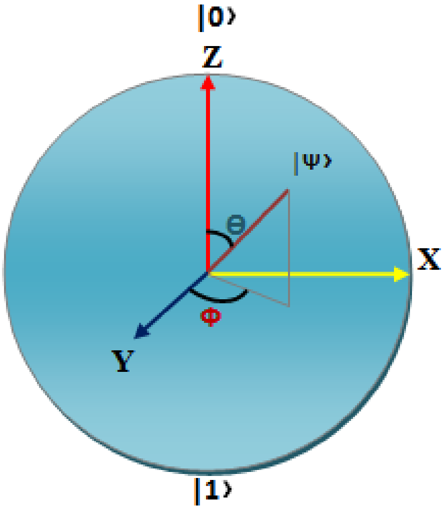


Figure 1.1: Bloch Sphere. The arbitrary representation of a Quantum State $|\psi\rangle$ with respect to the X, Y and Z basis

For instance, a quantum state $|\psi\rangle$ is present in a 3-dimensional Hilbert space $\mathcal{H}$ as shown in Figure 1.1. Hilbert space represents the complex vector space of a quantum system with an inner product (Young, 1988). It represents the exact position of a quantum state by measuring the phase and length by performing the inner product. The inner product is a process of multiplying two or more vectors to produce a scalar result. The operations will be performed on the quantum state if and only if it lies in Hilbert space. Let us assume the state $|\psi\rangle$ lies on one axis and makes an angle (θ, ϕ) with the remaining two axes as represented in Figure 1.1. According to this, the equation to measure a quantum state can be represented as follows.

$$|\psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle \tag{1.1}$$

Where θ, ϕ are real numbers and $0 \leq \theta \leq \pi$, $0 \leq \phi \leq 2\pi$. Bloch Sphere represents the quantum states $|0\rangle$, $|1\rangle$, which are known as spin-up and spin-down of a photon. The new pure state of a photon can be measured based on its position. As shown in Figure 1.1, a new quantum state $|\psi\rangle$ which is making an angle θ with Z-axis and ϕ with Y-axis can be measured using the equation 1.1. Here the value of $\cos(\theta/2)$ gives the possibility of state $|\psi\rangle$ becoming $|0\rangle$ and the value of $e^{i\phi}\sin(\theta/2)$ represents the possibility of becoming $|1\rangle$. The final state of $|\psi\rangle$ will be measured based on the higher probability. The equation 1.1 is further simplified as follows for performing operations.

$$|\psi\rangle = \alpha|0\rangle + \beta\,|1\rangle \tag{1.2}$$

Where α, β are the probabilities of state $|0\rangle$ or $|1\rangle$ such that $|\alpha|^2 + |\beta|^2 = 1$. Initially, a quantum state is in a superposition of both the states but once we measure it then it will be lost into any one of the states based on the maximum probability. Quantum states are also called basis vectors because these states are represented mathematically using vectors as $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$. The operations will be performed on multiple quantum states using the tensor product. For example, to implement a two-qubit state $|00\rangle$, the tensor operation will be performed on states $|0\rangle$ and $|0\rangle$. Which is expressed as follows.

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle \tag{1.3}$$

1.1.2 Entanglement

Quantum entanglement (Horodecki et al., 2009) is another special property of a qubit. A pair or group of quantum particles are said to be entangled if they are generated with similar properties and cannot be described independently. If the state of an entangled qubit is modified then it affects the other. With this, the data can be transmitted from one place to another without using any physical medium. Bell states are used to represent the entangled qubits. The total possible bell states with two entangled qubits ($|0\rangle$, $|1\rangle$)

in three-dimensional Hilbert space which are represented with the following equations and vector representations.

$$|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} \tag{1.4}$$

$$|\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix} \tag{1.5}$$

$$|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix} \tag{1.6}$$

$$|\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix} \tag{1.7}$$

As represented in the above equations, there are four possible ways for generating entanglement by keeping both the entangled qubits in same states with positive ($|\psi^{+}\rangle$) or negative ($|\psi^{-}\rangle$) phases as in equation (1.4) and (1.5) or in opposite states with positive ($|\phi^{+}\rangle$) or negative ($|\phi^{-}\rangle$) phases as in equation (1.6) and (1.7).

Entanglement plays a key role in various applications like secure communications, Quantum Key Distribution (QKD), etc. Moreover, it is a principal resource for quantum teleportation (Bouwmeester et al., 1997).

1.1.3 Quantum Teleportation

Quantum teleportation is a process of transmitting quantum information from one place to another using entangled qubits and classical communication. The process of teleportation is depicted in Figure 1.2.

As in Figure 1.2, for instance, if Sender (Alice) wants to share a piece of infor-

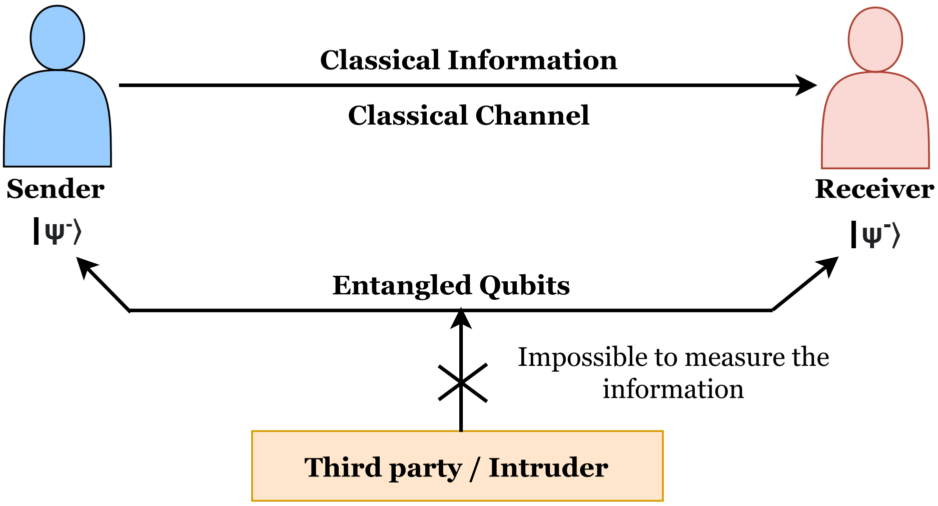


Figure 1.2: The process of Quantum Teleportation

mation with the Receiver (Bob) using a classical channel then there is a possibility of an attacker who can observe and modify the information. But suppose they use the entangled qubits for sharing the information by placing one entangled qubit at Alice's side and the other at Bob's side. In that case, there is no possibility for an attacker to observe or modify the quantum information due to the no-cloning theorem (Wootters & Zurek, 1982) and decoherence (Hornberger, 2009). According to these, if a person tries to measure the quantum state then its actual state will get disturbed and leads to errors or data loss. Thus it is impossible to copy the quantum data. Hence the data which is transmitted in the form of qubits are highly secured.

1.2 Reversible Operations

In classical computation, the operations which are performed are irreversible. i.e., if in case the input information is lost then it cannot be retrieved from the produced outputs. In irreversible operations, there will be n number of inputs and a single or less number of outputs (Li et al., 1998). According to Launder's principle (Landauer, 1961), the data loss with irreversible operations leads to the $\ln_2 kT$ Jouls of heat energy. Where k is Boltzmann constant, $\ln_2$ is the natural logarithm of 2 and T is temperature. i.e., the loss of every bit of information produces energy loss which in turn increases power consumption. To overcome this problem, Bennett (Bennett, 1973) has come up with a solution named reversible computation. In reversible computation, the number of inputs and outputs will be equal and each output is represented with a unique input combination. Even if we lose the information that can be easily retrieved from the output and leads to low power consumption. By taking this as an advantage, quantum performs reversible operations with quantum gates. There are various single and multi-qubit gates which are available to perform the operations in quantum computation. A detailed discussion of all these gates is presented in the following section.

1.3 Reversible Quantum gates

Quantum logic gates are used to implement the quantum logic circuits in order to perform the operations in quantum computing (Zulehner et al., 2018). The fundamental quantum gates with matrix representation are as follows.

1.3.1 Single qubit gates

Single-Qubit gate plays a vital role in quantum circuit implementation. These gates operate on a single qubit i.e., it accepts a single input and produces single output [14]. The single qubit gates which are used to produce superposition and to perform bit and phase shifts, etc are discussed as follows.

Hadamard Gate

It is the fundamental method for creating the superposition of a qubit. It performs the operation on a single Qubit i.e., it takes a single input and produces a single output. It represents the input state which is either $|0\rangle$ or $|1\rangle$ to a superposition of $|0\rangle$ and $|1\rangle$ with equal probabilities to become states 0 and 1. It plays a major role in many quantum circuits to generate superposition. It is graphically represented with the symbol H. Hadamard operation on a single qubit system with quantum states $|0\rangle$ and $|1\rangle$ can be represented as $H = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ for both positive and negative phases. Its matrix depiction is as follows.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.8}$$

Pauli gates

Pauli gates are represented based on the π angle rotation around the x, y, and z axis in the Bloch sphere. Based on the rotation over the axis, these gates are divided into three types Pauli X, Y, and Z gates which are explained along with these lines.

Pauli X gate

Pauli X gate performs the operations on a single Qubit. It is the same as a NOT gate in a classical computation hence it is also called a Quantum NOT gate. It is visually represented with the symbol X. If the input is given as $|0\rangle$ then X gate converts it into

$|1\rangle$ and $|1\rangle$ will be converted to$|0\rangle\rangle$. Hence it can also be called as a bit-flip gate. Its matrix representation is given below.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.9}$$

Pauli Y Gate

This gate accepts a single input and produces a single output. It represents state $|0\rangle$ to state i$|1\rangle$ and state $|1\rangle$ to state $-i|0\rangle$. It is pictorially represented with the symbol Y. Its matrix depiction is as follows.

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{1.10}$$

Pauli Z Gate

This gate performs operations on a single Qubit. After applying this gate on a qubit will not change the state if the input is $|0\rangle$, but if it is $|1\rangle$ then it will be modified to -$|1\rangle$. Due to this, it can also be called a phase shift/phase flip gate. It is pictorially represented with the symbol Z and its matrix representation is given below.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.11}$$

Phase Gates

Phase gates are used to represent the phase shifts while performing the operations. These are also single qubit gates. A phase gate is represented with the symbol $\mathbf{P}$. If the phase gate is applied on a qubit with $|0\rangle$ then it will be in the same state. But if the input is $|1\rangle$ then it will be modified to $e^{i\Phi}|1\rangle$. It means, it only modifies the phase of a qubit but the probabilities of $|0\rangle$ and $|1\rangle$ will not be modified. It changes the phase of a qubit along the Z-axis. The matrix representation of the phase gate with phase Φ is as follows.

$$\mathbf{P}(\Phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \tag{1.12}$$

Based on the phase (Φ) value the phase gates are divided into Z, S, and T gates. If a $\mathbf{P}$ gate is applied on a qubit then it rotates along Z-axis with phase $\Phi = 2\pi$. If $\Phi = \pi$ phase gate acts as a Z gate which is also called a Pauli Z gate.

S Gate

Phase gate acts as an S gate for $\Phi = \frac{\pi}{2}$. Its matrix representation is as follows.

$$\text{S gate} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{pmatrix} \tag{1.13}$$

If the phase is negative i.e., for $\Phi = -\frac{\pi}{2}$, then it is represented as $S^\dagger$ and termed as S-dagger gate. Its matrix representation is as follows.

$$S^\dagger\text{gate} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{i\pi}{2}} \end{pmatrix} \tag{1.14}$$

T Gate

Phase gate acts as a T gate for $\Phi = \frac{\pi}{4}$. Its matrix representation is as follows.

$$\text{T gate} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix} \tag{1.15}$$

If the phase is negative i.e., for $\Phi = -\frac{\pi}{4}$, then it is represented as $T^\dagger$ and termed as T-dagger gate. Its matrix representation is as follows.

$$T^\dagger\text{gate} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\frac{i\pi}{4}} \end{pmatrix} \tag{1.16}$$

U Gate

U gate also performs the operation on a single qubit and it is also called a parameterized gate. Till now we have discussed single qubit gates with two parameters δ, Φ, but the U gate is represented with three parameters δ, Φ, γ. Hence initially it is termed a U3 gate. Its matrix representation is as follows.

$$U(\delta, \Phi, \gamma) = \begin{pmatrix} cos(\delta/2) & -e^{i\gamma} sin(\delta/2) \\ e^{i\Phi} sin(\delta/2) & e^{i(\Phi+\gamma)} cos(\delta/2) \end{pmatrix} \tag{1.17}$$

U gate with parameters $(0, 0, \gamma)$ acts as a P gate and with parameters $(\frac{\pi}{2}, 0, \pi)$ acts as a Hadamard Gate.

1.3.2 Multi qubit gates

As of now, we discussed the gates which operate on a single qubit. To perform operations on multi qubits we need multi-qubit gates. Hence this section explains the various quantum gates which operate on two or more qubits.

Swap Gate

Swap gate is used to swap the qubits. It operates on two qubits i.e., it accepts two inputs and produces the two outputs as shown in Figure 1.3. If the inputs (I_{n1}, I_{n2}) of Swap gate are $|0\rangle$ and $|1\rangle$ then the outputs of this gate are $|1\rangle$, $|0\rangle$.

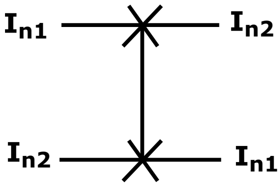


Figure 1.3: Graphical representation of SWAP Gate

Controlled-NOT Gate

This gate is also referred as CNOT gate and Feynman gate. It operates on two qubits i.e., it accepts two inputs called control and target inputs and produces two outputs called control and target outputs. For an example, consider the inputs of this gate as (I_{n1}, I_{n2}) and outputs as (O_{t1}, O_{t2}) as shown in Figure 1.4.

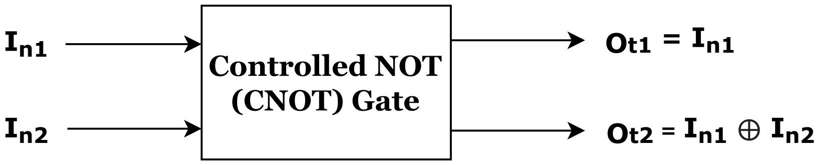


Figure 1.4: Graphical representation of CNOT Gate

As shown in Figure 1.4, the outputs can be retrieved from the equations $O_{t1} = I_{n1}, O_{t2} = I_{n1} \oplus I_{n2}$. The output of CNOT gate depends on the control input I_{n1}. If the I_{n1} is $|0\rangle$ then the outputs are the same as the inputs. Otherwise, if I_{n1} is $|1\rangle$ then the output O_{t1} is same as I_{n1} and O_{t2} is complement of I_{n2}.

Similarly, there are various multi-qubit quantum gates like Double Feynman gate, Peres gate, Toffoli gate, TR gate, and Fredkin gate are available to implement various quantum circuits.

1.4 Quantum Errors

The error rate is high in current NISQ-level quantum systems due to the noise and decoherence. The errors in classical and quantum computing are different because in classical, the possible errors are bit flip errors only but in quantum, the possible errors are three types Bit flip, Phase flip, and Bit & Phase flip which are explained as follows.

1. **Bit flip errors:** These errors are the same as classical bit-flip errors. When a bit flip error occurs in QIP, it modifies the actual quantum state. For an instance, the information need to be transmitted is $\alpha|0\rangle$+β $|1\rangle$. While transmitting it if any bit flip occurs then it converts the actual state into $\alpha|1\rangle$+β $|0\rangle$, where the qubits are modified.

2. **Phase flip errors:** Phase flip errors modifies the actual phase of the quantum state, i.e. if the quantum state is in a positive phase upon the occurrence of phase error, it will modify into a negative phase. For instance, the information needs to be transmitted is $\alpha|0\rangle$+β $|1\rangle$. While transmitting it if any phase flip occurs then it converts the actual state into $\alpha|0\rangle$-β $|1\rangle$, where the qubit phase is modified.

3. **Bit and Phase flip errors:** This error modifies both bit and phase of the actual quantum state. For instance, the information need to be transmitted is $\alpha|0\rangle$+β $|1\rangle$. While transmitting it if any phase flip occurs then it converts the actual state into $\alpha|1\rangle$-β $|0\rangle$, where the qubit and phase are modified.

Errors are mathematically represented with state matrices. Usually, the quantum states are represented with the state matrices with the combination of complex state vectors. The possibility of errors in quantum computing is high due to the delicacy of the quantum states. It results in noise and decoherence. In general, Quantum states are represented with a state matrix. A state matrix is a combination of complex state vectors. Let us assume ρ, $|\phi\rangle$ are the representations of a state matrix and a state vector. A new pure quantum state of these state matrices and vectors can be represented with the outer product of the state vectors as $\rho = |\phi\rangle\langle\phi|$. But after performing the operations on qubits, a pure quantum state will be modified as a mixed state due to the interaction with the external environment. This can be represented with the following equation.

$$\rho = \sum_{n} P_n |\phi_n\rangle\langle\phi_n| \tag{1.18}$$

Where P_n is the probability of quantum state $|\phi_n\rangle$. $|\phi_n\rangle\langle\phi_n|$ represents the vector inner product.

If we consider a quantum gate on a single qubit, the operation O_p will be performed with a unitary group of 2 states. Whenever the operations are performed on two states, the possible Pauli errors for all 4(2x2) states will be represented as follows.

$$O_p = E_I\Gamma_I + E_X\Gamma_X + E_Z\Gamma_Z + E_Y\Gamma_Y \tag{1.19}$$

Here $\Gamma_I, \Gamma_X, \Gamma_Y, \Gamma_Z$ represents the Pauli operators named identity, qubit shift, phase shift, qubit & phase shift. The matrix representation for these operators is given below.

$$\Gamma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \Gamma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \Gamma_Y = \begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}, \Gamma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

E_I, E_X, E_Y, E_Z are the probabilities with real and complex numbers such that $|E_I|^2 + |E_X|^2 + |E_Y|^2 + |E_Z|^2 = 1$

For error calculation, only X and Z errors will be considered. By considering these two we can also cover Y errors because of Y = XZ (McClean et al., 2020).

1.5 Error Correction mechanism in Quantum Computing

Quantum Computing has great potential compared to classical computing (Feynman, 1985). For example, the Shors factorization algorithm is exponentially faster than the efficient classical algorithms. Hence it is very important to ensure the accuracy of Quantum information processing. The theory of Quantum Error Correction(QEC) has been developed to protect the information from noise (Criger et al., 2012). With Quantum theory and practice development, Quantum circuits and experimenting with QEC approaches are achievable on platforms such as IBM Qiskit (Qiskit, 2019). Quantum Information Processing contains three steps in Quantum Computing. These are encoding the information, transmitting it through the Quantum channel, and finally decoding the information.

In Quantum computers, Quantum states can be easily affected by external noise; hence errors can occur at any time so the QEC techniques should protect the information while processing. Redundancy is added at the encoding side in the original information to handle the noise in advance. An error will be generated if the noise occurs during the information transmission. On the decoding side, the errors have to be corrected, hence the QEC technique has to perform encoding procedures in reverse order to correct the errors. This procedure contains error detection and recovery of the original information. The QEC techniques should satisfy two points, which are

i) Low Error Correction cost

ii) High Error Correction accuracy.

In QEC techniques ancilla qubits are used to protect the information. If fewer ancilla qubits are used, the error correction cost will be reduced.

1.6 Ancilla Qubits

The operations performed in a quantum computer are unitary transformations that conserve the inner product. It represents that the inner product of the vector must be unique before and after transformation. All the quantum operations are performed by implementing quantum circuits. While performing the operations, partial results will be generated. Due to the reversible operations, other than input and output we need extra qubits which can be used to perform the operations and store the partial results. Especially in Quantum error correction, to detect and correct the syndromes extra qubits are required. These extra qubits are called ancilla qubits or garbage qubits (Criger et al., 2012). Once the operations are completed, the ancilla qubits will be deleted. It will not increase the total number of qubits and does not affect the actual qubits. Ancilla qubits are initially represented with state $|0\rangle$. It reaches the same state after performing the operations. Ancilla qubits are used in various QEC techniques which are discussed in the next chapter.

1.7 Motivation

The features of quantum mechanics pave a path toward various approaches for transmitting information. The main problem observed in quantum computation is noise which is caused by unwanted interaction with the external environment. Therefore error correction methods play a crucial role in the quantum information process (QIP). Error detection and correction in quantum computation is a difficult task. Because as per the no-cloning theorem, copying quantum information is not possible. If one tries to do that, its actual state will be disturbed which leads to errors. As a solution to this, researchers working on developing quantum error correction techniques. From the literature, we observed that many of the existing works are symmetric in nature. The symmetric quantum error correction methods are implemented by considering the probability of getting bit and phase flip errors as the same but it is not the case. Furthermore, the probability of getting phase flip errors is more compared to the bit flips. Even after implementing the error correction methods, many authors (Shor, 1996; Tornberg et al., 2008; Riste et al., 2015; Wootton & Loss, 2018) concentrated on detecting and correcting only one error, i.e. either bit flip or phase flip at a time. However, it is important to find all the errors for efficient quantum error correction. In earlier days, the authors used to perform mathematical and theoretical operations to implement quantum architectures (Shor et al., 1998; Knill et al., 2000; Chiaverini et al., 2004; Cai et al., 2021). Due to the inbuilt noise of the quantum system, there will be differences between mathematical and quantum system outcomes. We can observe that by performing operations directly on quantum systems. Furthermore, optimized quantum circuits need to be implemented to design cost-effective quantum architectures. Hence these points motivated us to address the following issues:

- Efficient method for asymmetric quantum error correction to detect and correct bit and phase errors.
- Advantage of entanglement in quantum error correction to achieve better results.
- Effective and efficient utilization of cost-effective quantum circuits to develop Quantum cost optimization models.
- Designing and developing quantum algorithms on quantum systems to observe the exact outcome of the developed algorithms.
- Requirement of quantum error correction in various applications to overcome the drawbacks of classical computing.

Thus, the research in this thesis focuses on asymmetric quantum error correction by taking advantage of entanglement and developing optimized quantum architectures with the help of cost-effective quantum gates.

1.8 Summary

In this chapter, we discussed the fundamental concepts of quantum information such as superposition, entanglement, and teleportation. Further, the various single-qubit and multi-qubit quantum gates along with the concept of reversibility have been discussed. Also discussed the impact of various quantum errors on quantum information while transmitting in the form of quantum states. The importance of error correction in quantum computing and the role of ancilla qubits in detecting errors is presented as well.

1.9 Organization of the Thesis

The rest of the thesis is organized as follows.

In Chapter 2, an extensive literature review on existing quantum error correction methods and the observed research gaps are illuminated. Based on the outcome of the existing works, the problem statement and objectives are defined.

In Chapter 3, the scope of the proposed work and the research contributions are discussed, and also a brief description of the proposed methodologies for all the objectives is provided.

Chapter 4 presents a novel method for Entanglement Purification using Entanglement Swapping along with the result analysis of the proposed method with the existing state-of-the-art methods.

Chapter 5 presents an efficient method for Asymmetric Quantum Error Correction with Syndrome Measurement with and without using Entangled qubits. The result analysis with existing methods is also elucidated.

Chapter 6 presents the Quantum cost optimization model for the proposed asymmetric quantum error correction method along with the result analysis.

Chapter 7 presents the error correction in Quantum key distribution using the proposed method with result analysis.

Chapter 8 presents the concluding remarks of the presented research work and highlights the future research directions in this area.

Chapter 2

Literature Survey

In the previous chapter, we discussed in detail the fundamental concepts of Quantum computing like Superposition, Entanglement, Quantum errors and etc. The following chapter gives a detailed overview of the existing state-of-the-art methods on Quantum Error Correction, Entanglement Purification, Quantum Cost Optimization and Quantum Key distribution methods. The observed gaps from the detailed literature and the proposed problem statement along with the research objectives are also presented in this chapter.

2.1 Quantum Computing and Error Correction

Quantum computing is an advanced computation process that performs operations based on quantum mechanical principles. These principles made quantum computers exponentially more powerful, cost-efficient and energy-efficient than classical computers. According to the Church-Turing Principle (Church, 2003), Quantum computers can solve complex problems in exponentially less time than classical computers. It has been proved with Quantum Supremacy (Arute et al., 2019) by factoring integers in just 200 seconds, whereas the world's best supercomputer will take its lifetime to solve it. Even though Quantum computing has many advantages over classical computing but at the same time, it has some limitations due to the physical properties of Quantum particles. When we try to measure Qubit, it behaves like a particle and like a wave when it is not observed. Due to the dual property of a quantum particle, it is difficult to maintain coherence while performing the operations in a Quantum system. This leads to decoherence and noise which in turn leads to errors or data loss (Steane, 1996b). As a solution to these problems, error correction methods are to be implemented.

Quantum Error Correction plays an essential role in large-scale Quantum systems. Especially in the current NISQ era of quantum systems, the error rates are very high and the coherence time is very less due to the delicacy of the quantum particles. This makes building a Quantum computer with an error correction mechanism essential. The process of Quantum Error Correction(QEC) is different when compared to Classical Error Correction due to the following reasons.

- A Quantum bit is subjected to bit flip errors and to phase flips due to the fluctuations in its actual phase.

- As per the no-cloning theorem, it is impossible to copy the Quantum states.
- Measuring a qubit to detect the error will immediately destroy the Quantum states.

In classical computing, the data can be copied and measured but quantum information cannot be copied. Moreover, the information stored in the qubit may be lost if we try to measure it. This makes Quantum error correction a very challenging one. There are total three types of errors namely bit flip, phase flip and bit & phase flip errors as discussed in section 1.4. These errors frequently occurs in Quantum Information Process (QIP). QIP is a process of transmitting quantum information from one place to another. The significant steps to transmit the quantum information in QIP are depicted in Figure 2.1.

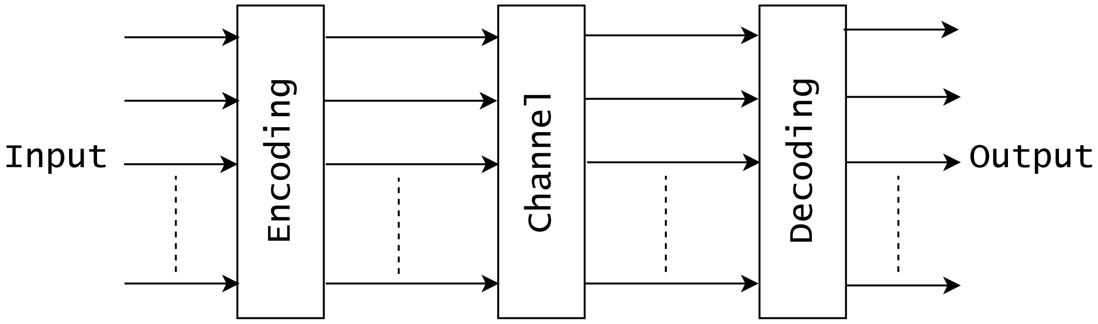


Figure 2.1: Steps in Quantum Information Process

Figure 2.1 shows three major steps in Quantum Information Process. The first step is encoding in which a logical qubit is protected by appending multiple physical qubits. The logical qubit is an actual qubit that needs to be transmitted from one end to another. It is difficult to find if any error occurs on the logical qubit as the actual qubit will be corrupted. In order to overcome this, we use extra qubits named as physical qubits which will be appended along with the logical qubit to protect the information as well as to detect and correct the errors. Once the data is encoded, it will be transmitted through the quantum channel. In a quantum system, optical fibre is used as a quantum channel. When the encoded data is transmitted through this channel, it has to interact with the external environment which results in errors. The resulting errors will be detected and corrected, the encoded data will be decoded into the original logical data by performing decoding operations. By following these steps, the authors developed quantum error correction methods using various approaches. A detailed discussion on the existing state-of-the-art quantum error correction methods are presented in section 2.2. The usage of entangled qubits in Quantum Error Correction leads to more accurate results and reduces the error rate. To apply entangled qubits, it is necessary to check whether the entanglement between qubits is maximal or not. If the entanglement is weak, it leads to more errors or data loss. In order to overcome this problem, entanglement purification techniques need to be performed. The detailed discussion on entanglement purification and the existing methods with merits and demerits are presented in section 2.3. In the current NISQ era of quantum systems, the requirement of cost and power-efficient quantum architectures are very high. Here the cost represents quantum cost. Quantum cost is measured based on the number of single and multi-qubit quantum gates used in the architecture. The usage of lowest-cost quantum gates to develop a quantum architecture leads to a reduction in overall cost which in turn leads to a reduction in power consumption. The detailed discussion on quantum cost optimization models, and the existing methods with advantages and disadvantages are presented in section 2.4.

2.2 Various approaches in Quantum Error Correction

Initially, the researchers (Bennett & Brassard, 1984; Peres, 1985) thought to apply classical error correction codes to perform error correction in quantum systems. The major challenge they observed here is the no-cloning theorem and orthogonality. In classical computing, multiple copies of the data can be maintained to protect it from errors. Even if an error occurs, it will be detected and corrected easily. But in quantum, it is not possible to maintain multiple copies of the data (Wootters & Zurek, 1982). Another essential property of quantum states is orthogonality. The quantum states must be orthogonal and normalized in order to maintain coherence. The quantum states are said to be orthogonal if and only if the vectors of the states are at a right angle. It is called normalized if the sum of its magnitudes is equal to 1. The orthogonality concept needs to be included to modify the classical error correction strategies into quantum models, which is quite difficult to implement (Hornberger, 2009). Thus till the early 90's, the researchers (Flynn, 1966; Pendry, 1983; Ebison, 1985; Josephson, 1988) felt that it is challenging to develop the error correction mechanism for quantum systems.

The first error correction code named quantum repetition code was introduced by Calderbank & Shor (1996) with reference to the classical repetition code in 1996. In this code, to perform error correction a single logical qubit will be encoded into three physical qubits by appending two extra qubits to the logical qubit with the same quantum state. To measure the error, two ancilla qubits were used. Based on the combination of ancilla qubits the errors will be measured. The main drawback is that if the error occurs on two qubits, it results in incorrect output. In order to overcome this problem, Shor et al. (1998) proposed a 9-qubit Shor's code. It will be used where a single logical qubit is encoded into nine physical qubits. Even though this performs better than the 3-qubit repetition code, there will be an increase in quantum cost due to the more number of qubits. Quantum cost represents the cost of a quantum circuit that is used to perform the operations with various quantum gates. Single and multi-qubit gates are used for the development of Quantum circuits. The cost of the quantum circuit is measured by calculating the cost of each gate associated with it. The 9-qubit Shor's code is further simplified into 7-qubit Steane's code (Steane, 1996a) which is also called as CSS code. This code uses seven qubits to perform error detection and correction. In this, a single logical qubit is encoded into seven physical qubits to detect and correct the quantum error. Later the additive codes are introduced (Gottesman, 1997). These codes stated that the minimum number of qubits required to perform error correction is 5. Along with these codes, Non-additive, Asymmetric and Entanglement assisted Quantum Error Correction codes were also introduced by the researchers which are explained clearly in the following sub-sections.

2.2.1 Additive Quantum Error Correction codes

Additive Quantum Error Correction codes are also called as Stabilizer codes which correct the local errors. Till 1997, most of the developed quantum error correction codes were stabilizer-based codes only (Cleve, 1997). The error correction process of stabilizer codes is depicted in the following Figure 2.2.

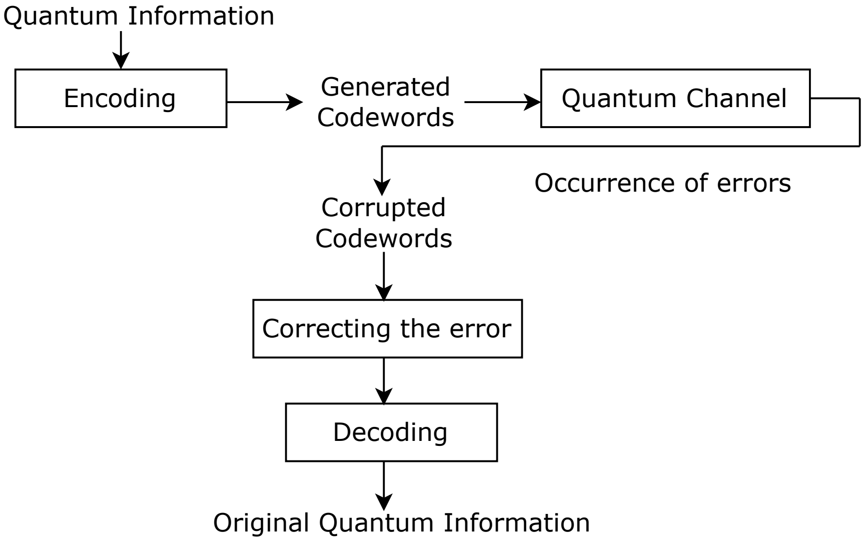


Figure 2.2: Error correction procedure in Additive Codes (Ezerman et al. (2011)).

As Figure 2.2 shows, additive code encodes the data into codewords. A codeword is a set of encoded states that are presented in code space. It can be represented as $|\psi\rangle \in \zeta$ where ζ represents the code space. It is a subset of Hilbert space $\mathcal{H}$ with n number of qubits, i.e. $\zeta \subseteq \mathcal{H}^{\otimes n}$ (Ezerman et al. (2011)). The generated codewords will be transmitted through the quantum channel. If any error occurs then the codeword will get corrupted. To detect and correct the error in a codeword, error correction methods will be applied. Once the error is corrected, the data will be decoded into the actual quantum information. Usually, a k-qubit quantum state will be encoded into n-qubit codewords. It means the extra (n-k) qubits are used to strengthen the qubit in order to resist errors. Along with these, the codeword distance is also considered for representing the error correction codes. The distance represents the distinguishable codewords, i.e. the number of codewords separated from each other. Let us assume the codeword distance is d. To detect minimum t errors the value of d must be $\geqslant t+1$. According to this, the code will be represented with the notation [n,k,d].

The authors Glaudell et al. (2016) proposed a stabilized Quantum error correction using the measures $[n,k,d]_D$ with level D=2. It is an improvised CSS code. In this code, the Quantum Non-Demolition (QND) measures are used to measure the erasure errors. The quantum noise will be added to the phase of a photon. Even after applying the noise, if the photon state is not modified during the measurement, then it is called a QND measurement. To measure the stabilizers of ancilla qubits, Quantum R gates and CPHASE gates are used. With this structure, the overheads are reduced compared to the non-additive codes. But by using R gates the cost of the quantum architecture will increase. The proposed model is efficient for Quantum repeaters.

Jackson et al. (2016) adapted the codeword-based stabilizer code framework to perform QEC. Moreover, the authors proposed Pauli error models for amplitude damping and phase damping noise using local Clifford gates. Here, amplitude and phase damping are possible noises in superconducting quantum systems. When the quantum states are transmitted through the amplitude or phase-damping channels, it leads to errors due to the existing background noise. To mitigate these errors, [6,4] measures are word stabilizers and word operators are used to perform error correction. The proposed method (Jackson et al., 2016) detects the single amplitude damping error or multiple phase errors using Pauli Kraus operators. Due to the asymmetry between the Pauli errors, the proposed method cannot perform efficiently on more qubits.

Ofek et al. (2016) implemented a full-fledged QEC by using the real-time feedback system. The real-time feedback is used to encode the data and monitor throughout the transmission for error occurrences. These errors will be corrected and information will be decoded. To perform these operations, cat code is used; moreover, the proposed method is hardware efficient. It extends the lifetime of a qubit to 320 microseconds from 180 microseconds. But it does not apply to traditional error correction methods even though it works extraordinarily on hardware-efficient architectures.

Pan & Nguyen (2016) proposed an error correction model for a 3-qubit system. This model performs the error correction and stabilization of a three-qubit repetition code using dissipation control. Dissipation control can be defined as the utilization of the energy of quantum states for required operations in spite of wasting it. With the help of the dissipation control, it is possible to perform the automatic quantum error correction by stabilizing the ground states. To do so, the tensor product operation will be performed on Hilbert space to model the errors using arbitrary error operations. The major problem with this method is detecting errors when two or more qubits are modified.

Roffe (2019) provided an overview of the implementation of various quantum error correction methods, fundamental concepts, and error correction and detection examples. The authors focused on the implementation of surface codes. Surface codes are dual-containing CSS codes that are defined on a 2D lattice. In this [4,2,2] code is used to detect the errors. To encode the information, multi-dimensional Hilbert spaces are considered for producing efficient results. Before encoding the information, a single qubit is parameterized into two-dimensional Hilbert space. After encoding the information, the qubit occupies four-dimensional Hilbert space to increase the accuracy. The proposed code was mainly used for detecting and correcting a single qubit error. If multiple errors occur at a time, it is difficult to find using this code.

Quantum Topological Quantum Error Correction codes (QTECC) were proposed by Chandra et al. (2017). To implement QTECC, authors performed the classical to quantum isomorphism. As we discussed earlier, classical codes cannot be applied directly to quantum systems. Based on the properties of quantum information the classical methods need to be modified and then applied on a quantum system. The authors implemented the classical-based quantum codes by including the orthogonality concept. After that to perform the error correction, quantum stabilizer codes formalism was used to reduce the Quantum bit error rate (QBER). It has achieved efficient results using [7,4,3] hamming bound. The proposed system's cost is higher than the existing works although the results are better.

The authors Babar et al. (2018) also discussed about the various designing principles of the duality of classical and quantum codes. Authors discussed that the Entanglement could be used to copy the quantum information and Hadamard gates are used to perform phase flips. But coming to the practical scenario, there are many problems that exist while performing the proposed operations like weak entanglement, noise, and decoherence. To store the measured information parity check matrices (PCMs) are used. The increase in the dimensions of the PCMs leads to an increase in the error rate which in turn leads to low efficiency.

Ahsan & Naqvi (2020) proposed re-configurable quantum error correction codes for the real-time errors using [7,1,3] transversal gates. Transversal gates are different when compared to the other quantum gates. A quantum gate is called as a traversal gate if it is possible to achieve a logical CNOT gate by applying a CNOT gate on each qubit. Traversal gates are beneficial in QEC for transmitting a logical qubit into physical qubits. In Ahsan & Naqvi (2020), authors implemented a decoupling transversal gate and applied that to decoupling transversal logical gate errors which are generated from state-preparation noise. The experimental results show betterment compared to the CSS codes. The role of CSS codes in Quantum key distribution for error correction is investigated by Jia et al. (2019). In this, the authors proposed a classical linear code-based quantum CSS code. They applied this in the BB84 protocol to perform quantum key distribution. The theoretical results show that the proposed method improves the security of the key.

Holmes et al. (2020) discussed the role of quantum error correction in boosting quantum computing power. The proof of the proposed concept is demonstrated using single flux quantum (SFQ) technology. This technology was used to avoid the decoding backlogs and this uses the T gates in order to increase the simple quantum volume (SQV) of quantum systems. A 5% of improvement is observed in decoder operations due to the reduced overheads. The overhead is calculated using the values of the error generation rate and decoder processing rate. To implement the proposed error correction model, T gates are used. T gate is also called as a phase gate with angle $\frac{\pi}{4}$. Due to the inbuilt system noise, if the phase fluctuations are more, it leads to more errors and decreases the quantum volume (SQV).

Li (2020) investigated various quantum error correction models. They categorized all the error models into discrete and continuous models. According to them, the performance of discrete error models like stabilizer codes, AQECCs, and EAQECCs was high compared to the continuous codes like direct continuous-time QEC (CTQEC) and indirect CTQEC. CTQEC error models correct the errors which occur continuously in time. They also discussed about the optimization-based error correction approaches in terms of fidelity and the importance of the perturbation error model in the present era of quantum systems.

Cane et al. (2020) quantified the lower probability bound for the transversal QECCs using low complexity repetition code and 7-qubit Steane's code. To perform the error correction, encoding needs to be performed. The authors used transversal CNOT gates and Clifford gates with the steane code stabilizers to encode the quantum states. A single transversal gate has been used in every error correction step instead of using multi gates. The use of multi-transversal gates will increase the circuit depth. This scheme has reduced the frame error rate in transmission. Unknown quantum states need to be encoded in order to implement fault-tolerant QECCs, which is not possible with the proposed scheme.

Roffe et al. (2022) introduced a novel framework for QEC based on the classical methods named as Coherent Parity Check (CPC) codes with a symmetric structure by implementing a parity check matrix for QEC. This method separates the coded Qubits into two types corresponding to the data register and the parity register. Based on these, the CPC scheme performed a round of cross-checks between the parity qubits for QEC at the decoder side using [10,4,1] qubits. It helps the researchers to apply the classical model on quantum to perform error correction. The main issue with the proposed method is to detect a single qubit error when more number of physical qubits are used. It increases the quantum cost and depth of the proposed CPC model.

Hanks et al. (2020) investigated the role of local variance in decoding the quantum information using surface and repetition codes. The authors claimed that the results would be improved by using local information while performing decoding operations. It also reduces the code distance and error rate. The authors applied Kolmogorov's Blossom V algorithm to reduce the logical error rate. The performance of the proposed model degrades when a depolarization channel is used for the information transmission. It is also observed that the impact of measurement error in QEC leads to high error rates.

Most of the QEC mechanisms are implemented based on imperfect parity check measurements which may return incorrect results or inject faults into the quantum states (Steane, 1996b). To overcome this, Shor (1996) introduced fault-tolerant error correction. The sequence of parity check measurements will be repeated until the same outcome is observed many times. The proposed fault-tolerant error correction takes the $\Omega(rd^2)$ time for the d-distance code determined by the r parity checks. To reduce the time complexity, Delfosse et al. (2021) proposed fault tolerance quantum error correction using parity check measurements. The authors achieved this by considering a noise model for parity check measurement by assuming that each codeword bit contains a bit flip error with an error rate of p. With the proposed model, the error correction can be achieved in $\mathcal{O}(dlogd)$ time. The proposed fault-tolerant error correction efficiently finds the errors in small codes, Low-density parity check (LDPC) codes, etc. But the proposed method works efficiently on bit flip error correction.

Cuvelier et al. (2021) proposed the QEC code using space-time block codes for non-coherent multiple-input multiple-output (MIMO) communication. The authors developed a framework to analyze the usage of QEC code in a non-coherent classical communication channel. Also developed a mathematical structure of quantum encoder to perform QEC in MIMO framework. Mathematically derived the decoder and compared the results with the coherent QEC models. To perform the experiments, an experimental setup is developed with multiple antennas and transmitters. Although the results are effective, space-time block codes restrict the number of transmitters and antennas to be equal or power of two. With this the bandwidth efficiency reduces.

Wagner et al. (2021) proposed QEC by estimating Pauli channels from the quantum syndrome measurements. In order to do that, the authors used stabilizer codes and Quantum data syndrome codes. Using Pauli channels makes it difficult to perform the operations due to the varying noise and fluctuations in the quantum phase. Quantum state decoherence is also a major reason for quantum errors. When the quantum state is in Hilbert space, it has to maintain coherence to protect the information stored in it. Once the coherence of the quantum state is lost, then the data stored in it will be lost or leads to errors. Martinez (2022) proposed a QEC algorithm to overcome the issue. Photonic qubits are used to develop the proposed QEC. An experimental setup is required to develop and perform the operations with photonic qubits. It performs efficiently in correcting errors but leads to data loss due to the very less lifetime of a photonic qubit.

From the above discussed papers, it has been observed that the additive codes perform the QEC operations using more number of qubits. When more number of qubits are used, the Quantum cost and depth will increase which in turn leads to an increase in the overall cost of the system and reduces the efficiency.

2.2.2 Non-additive Quantum codes

The non-additive codes are also called as non-stabilizer codes. These are implemented by combining multiple additive codes. The additive codes are implemented to correct the local errors using the classical linear codes. Non-additive codes are implemented based on the non-linear quantum codes to improve the parameters of Quantum Error Correction codes. The first non-additive quantum code is implemented by Rains et al. (1997) with parameters [5,6,2]. In 2008, Yu et al. (2008) performed experiments on non-additive codes and designed new codes with parameters [9,12,3]. This code corrects a single qubit error using a 12-dimensional subspace with a 9-qubit Hilbert space. The experimental results show that the [9,12,3] performs more efficiently than the stabilizer code of the same length to correct a single-qubit error. To design encoder and decoder circuits, the authors used Controlled Phase and Toffoli gates. Toffoli gate is a three-input and three-output gate with a quantum cost of 5 units. The overall cost and depth of the proposed QEC method are increased by using higher-cost quantum gates. The proposed architecture can be further optimized by using unit-cost quantum gates.

Smolin et al. (2007) discussed about the family of non-additive codes with code distance 2. Authors developed QEC code with parameters [n,3x2^{n-4},2] using Pauli operations. The proposed QEC code outperformed the existing codes when $n \geq 9$, but for $n \geq 11$ the performance of the code is degraded. Grassl & Beth (1997), Roychowdhury & Vatan (1998) examined various non-additive quantum codes and their impact on existing quantum codes. Lang & Shor (2007) proposed non-additive codes to prevent errors from the amplitude damping channel. This code performs the error correction using a self-complementary structure. The decoding architecture of this code does not perform syndrome measurement and recovery operations.

Grassl & Rotteler (2008) proposed Preparata and Goethal-based non-additive quantum codes. The Preparata and Goethals codes are rectangular codes and are described from the Data loss prevention (DLP) of the Bose–Chaudhuri–Hocquenghem (BCH) codes. Authors derived union stabilizer codes with parameters [5,6,2] from the stabilizer states. CNOT, Toffoli, X and Z gate operations are performed to encode the data. These codes were useful in higher-dimensional quantum systems. With the usage of higher-cost quantum gates, the quantum cost of the proposed error correction method increases. Ball & Puig (2021), Leditzky et al. (2022) discussed about the geometric framework of graphical non-additive codes.

From the literature, it has been observed that non-additive quantum codes are more difficult to implement than additive quantum codes, as they require additional qubits and more complex error correction procedures. However, they can provide better error correction performance in certain situations where independent errors on individual qubits are not the dominant source of error. Compared to the other error correction methods, non-additive codes require more number of parameters with that the cost of the quantum circuits increases.

2.2.3 Entanglement Assisted Quantum codes

The entanglement-assisted quantum error correction codes (EAQECC) perform the error correction using entangled qubits. Entangled qubits are used to reduce the effect of noise and errors on the transmitted information. Brun et al. (2006) discussed about the role of entanglement in correcting quantum errors. The authors proved that EAQECCs do not require dual-containing constraints. With this, it will be easy to implement EAQEC codes using classical linear codes. Wilde et al. (2007) proposed continuous variable EAQEC code with linear optics. Entangled qubits are used to encode the information and recover the errors. In this EAQEC, optical elements are used to implement the encoder circuit. For large applications, the proposed QEC algorithm requires more number of squeezers to construct an encoder circuit. Squeezer states are used to maintain the uncertainty between quantum states.

Wang et al. (2019) proposed Quantum Maximum Distance Separable (QMDS) code for error correction. q-ary QMDS codes have a minimum distance of length $n = q^2 + 1$. A detailed investigation on EAQEC codes with length $n = q^2 + 1$ was also presented. In the proposed EAQEC, more number of entangled bits are required if the minimum distance between code words is larger. Due to this, the flexibility to generate entanglement between qubits will be improved.

Matsumoto (2020) presented the Gilbert-Varshamov (GV) -Type existential theorem for Entanglement Assisted Quantum error Correction (EAQEC). GV bound performs the direct products of two linear spaces and Euclidean inner product to detect and correct the error. In this code, they used an entangled pair in QIP to transmit the information. The method gives efficient results when compared to the GV-type EAQEC.

When the entangled qubits are used in error correction, there will be a possibility of generating weakly entangled qubits. In such cases, the error rate increases, leading to data loss. In Matsumoto (2020), authors didn't discuss about the weak entanglement and the steps to overcome this problem. The authors Şahinkaya et al. (2022), Allahmadi et al. (2022), Sidana & Kashyap (2022), Chen (2022) proposed novel architectures for EAQEC codes with local rings, arbitrary lengths & distances and singleton bounds. All these codes are implemented based on the GV bound. They also investigated the possibility of combining multiple codes to develop an efficient code.

Fan et al. (2022) proposed an Entanglement-Assisted Concatenated Quantum Code (EACQC) by concatenating two different quantum error correction codes. When the multiple quantum codes are combined, the non-degenerated hamming bounds will be violated. EACQC outperforms Concatenated Quantum Code (CQC) and corrects the error that is occurred on ebit. The authors Grassl et al. (2022) extended the existing EAQECs by including the singleton bounds. In this, they used Catalytic QECCs along with EAQECCs. To develop these codes, block length and distance between qubits are considered. If the distance between qubits is more then the proposed method may not detect the errors properly. The increasing distance weakens the entanglement between qubits. As a solution to this, authors Ouyang & Lai (2022) proposed EAQECCs with linear programming bounds. Linear programming bounds are mainly used to implement non-trivial upper-bound quantum codes and will not be suitable for detecting all types of errors.

From the literature, it is observed that the EAQEC codes perform well. But when we depend entirely on entangled qubits, the error rate and the possibility of data loss increase. The major problem we encounter in EAQEC codes is the external noise due to which the entanglement between qubits becomes weak. In QIP, the data has to be transmitted to longer distances. In such cases, the error correction using entangled qubits will degrade the efficiency because maintaining the entanglement between the two parties across greater distances is challenging.

2.2.4 Asymmetric Quantum codes

In asymmetric quantum error correction, the quantum information is encoded in a way that makes it more resilient to certain types of errors, while other types of errors are more easily correctable. In quantum computation, the possibility of getting phase flip errors is more due to the phase fluctuations in quantum states. In such cases, it is essential to concentrate more on phase-flip errors. However, Asymmetric Quantum Error Correction Codes are used to detect and correct both bit and phase flip errors but gives more priority to phase flip errors. The authors Chiani & Valentini (2020a) proposed generic Pauli error correction using stabilizer codes. Most of the existing QEC methods are designed to correct generic errors. Generic errors are the combination of Pauli operators like X, Y, and Z. The authors used [9,1] stabilizer code to detect and correct Z-type Pauli errors. [9,1] stabilizer code performs efficiently when there is an asymmetry between quantum channels. The proposed method used a generic hamming bound to define the minimum distance between the codewords while performing the error correction. With this modified hamming bound, the proposed error correction method shows efficient results than the [13,1] code (Ma et al., 2019). If the code word distance is less, the performance of the proposed generic Pauli error correction code degrades. With [9,1] stabilizer code, the quantum cost and depth of the proposed architecture increases.

Lv et al. (2021) proposed AQECCs using Quasi-Cyclic (QC) construction. Quasi-cyclic codes are generated from the cyclic codes. QC codes are one of the good AQECCs over small fields. The authors discussed r-generator-based QC codes and the dual-containing representation of 1-generator-based QC codes. The authors also embedded the QC codes into 2-generator-based and 3-generator-based QC codes. The major limitations of the QC codes are as follows: The maximum number of errors that can be corrected by a QC code is limited by its distance. QC codes can able to correct errors that occur on a subset of the qubits in the encoded state. This means the errors that occur on the remaining qubits will not be corrected, and the encoded quantum information will be lost. These limitations reduce the performance of the QC codes compared to the existing AQECCs.

Authors Roffe et al. (2022) proposed bias-tailored Low-Density Parity Check (LDPC) codes. LDPC code is an alternative error correction code to surface code. LDPC codes are playing a major role in implementing fault-tolerant quantum systems. LDPC codes have advantages over the existing quantum codes and at the same time, it has some limitations. Usually, LDPC codes are also called as a family of multiple codes with more number of qubits. Even though it is showing excellent results theoretically, it is difficult to say when good LDPC codes exist while doing the experiments with the quantum states. The bias tailoring operation performs the QEC by considering the asymmetry between quantum errors. The proposed method modified the existing surface code with Pauli operators XZZX with biased noise. The theoretical results show that the bias-tailored LDPC codes perform efficiently in depolarizing noise channels. But practically, it is difficult to bias the quantum phase noise.

Sundaresan et al. (2022) proposed a fault-tolerant syndrome extraction protocol by developing a decoder with a real-time feedback system. The experiment was performed on superconducting qubits which are connected in a heavy-hexagon lattice. The logical error is reduced with the proposed decoder. The major problem observed here is the possibility of sampling error which is increased with the proposed real feedback system. Most of the existing fault-tolerant architectures are implemented by using Clifford gates. Ryan-Anderson et al. (2021) proposed fault-tolerant QEC with [7,1,3] code and without using Clifford gates. The encoder and real-time decoder perform efficiently in detecting and correcting quantum errors. The proposed method requires seven qubits to correct a single qubit error. With this, the quantum cost and depth of the architecture increases.

The author Fuentes (2022) discussed about the Quantum Low-Density Generator Matrix (QLDGM) CSS codes for depolarizing quantum channels. QLDGM code gives efficient results compared to the Quantum low-density parity check (QLDPC) codes. But with the increasing complexity of QEC, it is difficult to optimize the Quantum Bit Error Rate (QBER) for asymmetric quantum channels. Initially, surface codes are designed for the symmetric error channels. But Azad et al. (2021) modified the surface code so that it can work in asymmetric quantum channels by measuring pseudo threshold values. This code performs the operations with less number of qubits compared to the existing works.

Fan et al. (2021) amalgamated Concatenated Codes (CCs) and Tensor Product Codes (TPCs) to develop Asymmetric quantum concatenated and tensor product codes (AQCTPCs). The Concatenated Codes are able to find phase-flip errors and TPCs are able to find bit-flip errors. Combining these two codes makes it possible to correct both bit and phase flip errors. The AQCTP codes perform the inner and outer product operations using different codes. Because Tensor Product Codes are developed by performing inner and outer products using different quantum codes. AQCTPCs are highly degenerative codes. Thus they can passively correct the bit flips compared to the phase flip errors. In Fan et al. (2021) authors focused on quantum decoder circuit architecture. To improve the performance of the encoder circuit, the authors Fan et al. (2021) proposed Asymmetric Quantum Concatenated codes (AQCCs) with a novel encoder circuit to detect and correct degenerative errors.

Apart from the above-categorized codes, other QEC codes like Binary QEC codes, Non-binary QEC codes and Coherent Parity Check (CPC) codes were also discussed by the authors Sarvepalli et al. (2009); La Guardia (2013); Ezerman et al. (2013); Verma et al. (2022); Pang et al. (2022); Kuo et al. (2022). The authors Aly (2008); Ezerman et al. (2013) investigated on the logical errors and proposed techniques to mitigate logical errors. Along with the logical errors it is also crucial to discuss about physical errors. While performing the error correction the possibility of data leakage is more. During the computation, if the qubits are at high energy levels then those may excite and leads to the leakage of information. As a solution to this, McEwen et al. (2021) investigated on the leakage during the error correction and proposed a reset protocol to reset the qubit from a higher level to ground level. In order to implement this, a bit flip stabilizer code was used. Bit flip stabilizer code is a simplified version of the surface code. The proposed method leads a path towards scalable computing, but the proposed method is helpful for finding only bit-flip errors. Even it is difficult to use reset protocols in practical QEC with the correlated nature of the leakage-induced errors.

Cao et al. (2022) developed a variational quantum algorithm to search cost-effective quantum codes. This algorithm can find QEC codes for any error model like pure or impure, degenerate or non-degenerate, etc. Fuentes (2022) also investigated various quantum codes and proposed sparse codes for error correction. Sparse codes are implemented by taking the base of classical error correction codes. Khalifa et al. (2021) discussed the digital design of QEC. The authors discussed about 9-qubit Shor's code and developed a modified QEC circuit by adding Hadamard gates to the existing one.

Convy et al. (2022) proposed a machine learning algorithm for the continuous QEC based on the Recurrent neural networks (RNN). The proposed algorithm identifies the bit flips from the continuous syndrome measurements. The results of this algorithm are compared with the double threshold scheme and Bayesian classifier. After comparing the results, it has been observed that the proposed algorithm outperforms the existing methods.

Das et al. (2022) developed a Lightweight Low-Latency Lookup-Table (LILLIPUT) decoder for QEC. It mainly performs two operations. They are - First, it converts syndromes into error detection events and those will be stored in the Look Up Table (LUT). Next, LUTs will be programmed with error assignments to find the errors. LILLIPUTs will be programmed on FPGA and utilizes the 7% of logic space on FPGA. The model currently concentrates on detecting bit flips only. It can be further extended to find all types of errors. Bhoumik et al. (2021) proposed a two-level decoding method for QEC using machine learning. From the results, it has been observed that the proposed method shows an excellent performance with the train and test ratio.

From the extensive literature, it has been observed that the AQEC with entangled qubits (ebits) produces better results and also provides more security while communicating the data. Thus the AQEC can be performed with qubits and ebits for efficient results. When the entangled qubits are used, it is necessary to check whether the entanglement between qubits is maximal or not. If the qubits are weakly entangled, it leads to more errors and data loss. To develop maximally entangled qubits, entanglement purification techniques need to be performed. A detailed discussion on Entanglement Purification and the existing EPPs is presented in the following sections.

2.3 Entanglement purification

Entanglement is a principal resource for various applications like secure communication, quantum error correction, QKD, etc. The entangled qubits will be shared between multiple parties to perform operations like data transmission, key distribution and etc. The critical question here is whether an entangled qubit is secured from the inbuilt noise. Noise weakens the entanglement between qubits. In order to overcome this problem, entanglement purification techniques are introduced. Entanglement purification is a process that is used to generate highly entangled quantum states that are resistant to noise and other forms of error. There are several different entanglement purification methods have been developed to date which are discussed below.

Yan et al. (2022) proposed Measurement-based Entanglement Purification Protocol (MBEPP) for the entangled coherent states (ECS). This protocol distils the strong ECSs from a large number of weak ECSs. The bell states are used to measure the entanglement between the qubits. MBEPP was implemented based on the Quasi-bell states. Quasi-bell states are introduced by Horoshko et al. (2019). Quasi-bell states are explicitly entangled coherent states and are used to measure the entanglement between coherent states. In MBEPP, to generate entanglement between coherent states GHZ method has been used. Behera et al. (2019) also proposed an EPP using GHZ states and experimented with it on the IBM quantum system. The entanglement between GHZ states is measured using Schmidt decomposition. Schmidt decomposition is a mathematical tool used for understanding a quantum state's entanglement structure. It is also used to identify and eliminate errors in the quantum state. Due to the high degree of entanglement, GHZ states are sensitive to noise and other forms of error. This can make it difficult to maintain the integrity of the quantum state over time. This can limit their usefulness in certain applications.

Liu et al. (2022) proposed a two-way entanglement purification technique for quantum key distribution. Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) provided the quantum key security proof using coherent quantum states and estimated the result in terms of error rate and photon gain. To prove this, a two-way entanglement purification protocol (EPP) is used as it performs efficiently and reduces the bit and phase error rate. The problem observed here is weak coherent states. To perform the experiment, authors considered coherent states. With weak coherent states, the results will be degraded.

Yin et al. (2022) developed an entanglement purification technique for polarization-entangled photon pairs using heralded high-fidelity parity-check detectors (PCDs). These are constructed by double-sided quantum-dot-microcavity (QD-microcavity) systems and linear-optical elements. In this method, spin states are used along with quantum states to perform entanglement purification. It generates the entanglement between a mixture of the various quantum states and can be very useful in quantum networks. With the proposed EP method, it is difficult to maximize the fidelity after a certain range.

To improve the fidelity, Lu et al. (2020) developed an EPP for mixed states with bit and phase flip errors using the Controlled Phase Flip gate (CPF). CPF gates perform efficiently in purifying the entanglement between two quantum systems in long-distance communication. CPF gates reduce resource consumption but the problem of double-sided optical cavities increases with the photon emission in real-time quantum systems. While working with EPP, it is also important to consider the phase fluctuations that arise while performing the operations on qubits. For that, Zhi & Zheng (2020) investigated the effect of phase fluctuations in entanglement purification. According to them, this problem can be reduced by dividing the convergence pattern of the initial quantum states into two regions. Convergence patterns are used to measure the degree of the electron beam. The fractal-like framework is used between these two regions to purify the entanglement into maximally entangled states (MES). The number of iteration steps used to perform these operations must be less; otherwise the quantum cost increases.

Till now, the discussed EPPs distil the high-quality entanglement from low-quality entangled states in the same ensemble. The authors Zhou et al. (2020) proposed a purification protocol that purifies the entanglement of the quantum states which are in different ensembles. Ensembles describe the group of entangled states which are in the same bell pair, i.e. either in $|\psi\rangle^+$ or $|\phi\rangle^+$. Proposed EPP performs operations on different ensembles, i.e., on both $|\psi\rangle^+$ and $|\phi\rangle^+$. These are also called mixed entangled pairs. The entanglement between different ensembles on mixed quantum states leads to phase flips and degrades the entangled pair's fidelity. Moreover, the performance of the different ensemble EPP needs to be investigated on the measurement-based EPP.

Chuu et al. (2021) discussed the purification of single and entangled photons using wave-packet shaping. Wave-packet shaping is a quantum optics tool that is used to manipulate the wave functions of single and entangled photons. To perform the experiments, colloidal quantum dots are used at room temperature. With the results, it has been observed that the wave-packet shaping method gives better results compared to the non-degenerate entangled pairs and spatial entanglement. The proposed EPP is hardware efficient and requires a special setup to perform the entanglement purification.

The authors Huang et al. (2022), Lu et al. (2022) proposed one step polarized entanglement purification method using spatial mode entanglement. The existing EPPs are implemented to purify the entanglement using at least two pairs. But a single pair of the hyperentangled qubits are used in the proposed experiment. Hyperentanglement is a type of entanglement between quantum states with multiple degrees of freedom (DOF). The proposed method shows efficient results in spatial mode. For time-bin entanglement, the results are degraded because of multiple DOF. Even in practical communication, the noise which is generated due to the environmental interaction leads to multiple DOF. It results in various effects which in turn leads to errors or data loss.

The authors Ghosh et al. (2018); Hu et al. (2021) proposed entanglement purification using hyperentangled states. Instead of using two entangled pairs, single hyperentangled pair is considered for performing entanglement purification. To generate hyperentangled pair a specific experimental setup is required where the light beam is used to generate the quantum states. Hadamard and CNOT operations are performed on these quantum states to prepare hyperentanglement and reduce QBER. This experiment is hardware dependent and can be improvised to utilize it in applications like quantum repeaters, QKD, etc. Most of the existing EPP used spatial mode entanglement but time bin entanglement also plays an important role in EPPs. Time-bin entanglement (Sheng & Zhou, 2014) is a type of entangled quantum state that is characterized by a high degree of entanglement between two modes of a single photon. These modes can be considered as ”time bins,” corresponding to different time intervals.

Yan et al. (2021) proposed EPP based on time-bin entanglement. Time bin entangled qubits are ideal for long-distance communications. Spontaneous parametric down-conversion (SPDC) sources are used in the realization of the EPP. The noise emitted from the SPDC source can be eliminated automatically. The CNOT or similar gates are used in existing EPPs to generate entanglement. In the EPP, feasible sum frequency generation (SFG) is used. Feasible sum frequency generation (SFG) (Landes et al., 2021) is a nonlinear optical process that involves the combination of two or more optical frequencies to produce a new frequency. Time bin entanglement gives high generation rates and can be proficient in various applications compared to spatial mode entanglement. The proposed EPP is hardware dependant. Time bin entanglement requires a complex experimental setup involving beam splitters, detectors, and other specialized equipment. This can make it challenging to implement and may limit its practicality in certain applications.

Luo et al. (2021) proposed multipartite entanglement purification protocol (MEPP) using time-bin entangled pairs. The GHZ states are used to generate the entanglement between quantum states. Generally, in MEPP two polluted entangled pairs will be used and those will be purified using purification techniques. Unlike these, the proposed MEPP requires a single pair of noisy time bin hyperentangled qubits to purify the entanglement. With this, the efficiency of the proposed EPP will be increased but if time bin and polarization DOFs occur on different types of photons, then the EPP can correct only the bit flip errors even though there exist phase flip errors.

Zhou & Sheng (2021) developed a 2-step EPP for the polarization entanglement using single hyperentangled states in spatial, time bin and polarization DOFs. Initially, the purification process will be performed on two identical quantum pairs. In this step, the bit flip errors will be purified. To purify phase flips, Hadamard operations were performed. If the purification step fails, then it leads to mixed quantum states. To purify the mixed quantum states, photon detectors will be used in the second step. This step generates highly entangled qubits. The proposed method increases the fidelity of the entangled pairs. But if both steps fail, then it leads to residual entanglement. It is also difficult to generate multiple hyperentangled pairs simultaneously.

To protect the entangled qubits in quantum networks, Yan et al. (2022) proposed EPP using optical fibre channels. While transmitting the entangled qubits through the optical fibre-based quantum channels, noise will be generated. It leads to amplitude damping errors that degrade the entangled qubits' fidelity. To distil the highly entangled pair from weak ones, authors used frequency bias pulses in EPP. These pulses purify the entanglement. It performs efficiently for meter-scale quantum networks. If the distance is more, the performance of the proposed EPP degrades.

Ecker et al. (2022) discussed the establishment of polarization-based entanglement over the noisy quantum channels. In this entangled pair, one DOF will be remotely transferred to the other DOF through the noisy channel. Multiple DOFs are entangled using CNOT operations. It provides versatility in entanglement transfer. To develop and experiment with EPP, a specific setup with photon detectors and light emitters is required. Xu et al. (2022) discussed the use of Quantum neural networks (QNN) for entanglement purification. The authors applied QNN to reduce the noise. Here the noise is divided into unitary and non-unitary noises based on the depolarization and amplitude damping noise. From the experiments, it has been observed that fidelity improves in non-unitary noise channels. But when it is applied in the depolarization channel, the results are degraded.

From the detailed literature, it has been observed that most of the entanglement purification methods are implemented using GHZ states. With the Schmidt decomposition, the GHZ entangled states will become separable. It weakens the entanglement between quantum states which leads to data loss. It is also difficult to generate the entanglement between a large number of qubits using GHZ states. GV bound, hyper-entanglement, time bin, or spatial mode entanglement were also used for developing EPP. These methods increase the phase fluctuations. In order to develop an efficient quantum architecture, it is essential to optimize the quantum cost. Otherwise, the cost of the entire system increases and that leads to more power consumption.

2.4 Quantum Cost Optimization

Quantum cost optimization is a method for minimizing the number of quantum resources to implement a quantum algorithm or perform a specific task. It is important as quantum resources are often limited and expensive, and minimizing their use can reduce the overall cost and complexity of quantum architecture. Quantum computer performs reversible operations. The importance of reversible computation has increased with emerging technologies. According to the Launders principle (Landauer, 1961), irreversible operations lead to energy loss. The loss of information in irreversible computation will generate the $\ln_2 kT$ Jouls of heat energy. Where k is the Boltzmann constant, $\ln_2$ is the natural logarithm of 2 and T is the temperature. With the development of reversible computation (Bennett, 1973), it became easy to perform various operations that are difficult with classical computation. Operations like Super dense coding (Harrow et al., 2004), Entanglement (Horodecki et al., 2009) and Quantum teleportation (Bouwmeester et al., 1997) are not easy to perform with classical computation but made easy with reversibility concept. The reversibility concept is the major advantage of quantum computation. Conventional computer performs irreversible operations. With this, the input bits will be lost once the output is generated. The classical gates like AND, OR, NAND, NOR, and EX-OR are multi-input and single-output gates and are not reversible (Caves, 1999). A logical gate is called reversible if and only if it contains an equal number of inputs and outputs. In this each output is represented with a unique input combination. The inputs can be restored easily even after generating the outputs (Nielsen & Caves, 1997). The energy-efficient reversible gates are used to implement reversible circuits in quantum computation. These circuits play a crucial role in applications like Optical computing, Nanotechnology, Secure communications, etc. Where the need for extremely low power consumption is desirable (Razeghi, 2010).

The reversible logic operations run the system in both forward and backward directions. This helps to generate the input information from the retrieved outputs. The energy dissipation will be reduced or sometimes eliminated with lossless operations in reversible computing. Various reversible gates like Fredkin (Patel et al., 2016), Feynman (Remón et al., 2009), Peres (Donald & Jha, 2008), Toffoli (Fedorov et al., 2012) gates etc., exist in literature. The computational complexity of reversible logic gates is often represented by Quantum cost. Quantum cost represents the technological cost to build any quantum circuit or architecture using single as well as multi-input gates. The quantum cost of single input and single output gates is equal to 1 unit. Quantum cost increases with the increasing number of inputs and outputs. The reversible circuits are optimized by replacing the multi-input and multi-output gates with a single or fewer number of input and output gates. Quantum cost optimization models were implemented by many authors for reversible sequential circuits (Wille et al., 2010), Shor's algorithm (Paler & Basmadjian, 2022), decoder (Slimani et al., 2022), dense coding (Qiu & Chen, 2022) and many more. The importance of quantum cost optimization methods has increased for the development of energy and cost-efficient architectures.

Quantum cost optimization is essential to build cost-effective quantum circuits.

Quantum cost represents the technological cost to build any quantum circuit or architecture. Mamun et al. (2014) proposed quantum cost optimization model for reversible sequential circuits like latches, SR & JK flip flops. Feynman gate (FG), Double Feynman gate (DFG), and Modified Peres Gate(MPG) were used to optimize the sequential circuits. Szyprowski & Kerntopf (2011) proposed an optimization method for four input and four output gates. The optimization can be performed by splitting multi-input Toffoli gates into Smaller size Peres gates or CNOT gates.

The authors Basak et al. (2019) developed a cost minimization method using the merger rules of the Exclusive Sum of Product(ESOP) method. K-maps are considered along with various gates like CNOT gate, Peres gate, TR gate, and Mixed Polarity Multiple Control Toffoli (MPMCT) gates. MPMCT gates gave an efficient result for large-size reversible circuits. Maity et al. (2020) proposed an optimized cost architecture for 2x4 decoder using reversible logic blocks. Similarly, the authors Maity et al. (2018), Montaser et al. (2015), Heranmoy et al. (2018), Ali et al. (2015), Majumder et al. (2015), Mohammadi et al. (2008), Kheirandish et al. (2021), Slimani et al. (2022) proposed quantum cost optimization models for 4-bit reversible universal shift register, decoder, BCD to excess-3 code converter, Memory circuits, Comparator, adder and subtractors using Peres and Toffoli gates. Pandey et al. (2022) proposed an optimized circuit for Arithmetic Logic Unit using reversible gates. Wang & Wilde (2020) discussed about quantum entanglement cost simplification with the help of properties like additivity and faithfulness. The authors developed the cost simplification method for the mathematical scenarios but not applicable to physical experiments and cost calculation methods were also not discussed.

Hogg & Portnov (2000) developed a quantum cost optimization algorithm for the travelling salesman problem and satisfiability problem. This algorithm shifts the amplitude from higher-cost states to lower-cost states in order to reduce the cost of the model. The proposed work gives an efficient result for smaller instances. Banerjee & Pathak (2009) proposed quantum cost optimization circuits for quantum teleportation, EPR pair, and decoders using mathematical calculations. In all the architectures, Toffoli gates were used. The quantum cost of Toffoli gates is more. The overall cost would have been reduced if the authors had used single-unit cost gates instead of Toffoli gates. Banerjee (2010) proposed cryptographic architecture using optimized reversible gates. For this, they used Toffoli and CNOT gates. Qiu & Chen (2022) proposed an optimization algorithm for quantum teleportation and super dense coding using Hadamard and CNOT gates. To calculate the quantum cost and optimize it, mathematical operations were performed using U, H, and CNOT gates. Feng et al. (2022) discussed the parameterized quantum circuits for teleportation.

From the literature, it has been observed that most of the optimized circuits are proposed using Toffoli and Peres gate. Toffoli and Peres gates are three input and three output gates with a quantum cost of 5 units. These gates can be replaced with single-unit cost gates like CNOT, Hadamard, U, S and T gates to reduce the cost and optimize the architecture. The optimized architectures of Entanglement Purification and Quantum error correction are very useful in applications like Teleportation, Secure communication and Quantum key distribution(QKD). QKD is a secure communication protocol that uses quantum states to generate a key for secure data communication. The existing QKD protocols and their limitations are discussed in the following section.

2.5 Quantum Key Distribution

Quantum key distribution (QKD) is a method for securely distributing cryptographic keys between two parties using the principles of quantum mechanics. It allows two parties to communicate securely by generating and exchanging a shared secret key. This key can be used to encrypt and decrypt messages. The security of QKD is based on the fundamental principles of quantum mechanics, which make it impossible for an eavesdropper to intercept and measure the key without introducing detectable errors in the system. This allows communicating parties to detect any attempts to intercept the key and take steps to protect their communication. Several different quantum key distribution (QKD) protocols have been developed over the years, which are discussed as follows.

Bennett (Bennett & Brassard, 1984) proposed the first key distribution protocol named as BB84 protocol based on the Einstein-Podolsky-Rosen (EPR) (Song, 2004) and Clauser-Horne-Shimony-Holt (CHSH) (Bruß, 1998) experiments. BB84 protocol was implemented to transmit the information between two parties like Alice and Bob safely using classical and quantum channels. The key was generated using a polarization basis and can be transmitted through the quantum channel. Both the communicating parties discuss about the key through the classical channel. The actual quantum state will be modified if an attacker tries to measure the key. The state modification will be known by the communicating parties by which the new key will be shared. BB84 protocol is proved to be the best method for secure communication. Ekert Ekert (1992) re-proposed the protocol and named it as E91. Once the E91 has come into existence, the actual quantum key distribution era started. In 1992, the first experimental demonstration was performed and in the same year, B92 QKD protocol Bennett (1992) was proposed. In the BB84 protocol, four different polarization basis were used for generating the quantum key but B92 proved that two different basis are sufficient for generating a secure key.

The authors Gisin & Pellaux (1992); Guo et al. (2006); Dušek et al. (2006) reviewed various QKD methods and their limitations. In 2002, the authors Gao (2008); Honjo et al. (2008); Ji et al. (2022) presented about the role of entanglement swapping in quantum key distribution. It is also observed that the entangled pairs play a crucial role in QKD for secure key transmission. The entangled qubits are mainly used to transmit the data for longer distances. The QKD protocol proposed in Ribordy et al. (2000) produces the 8.6% error rate using the Franson-type setup which was used to monitor the quantum correlations between the entangled qubits. The trusted party and untrusted party QKD protocols were proposed by the authors Yin et al. (2017); Peloso et al. (2009); Shi et al. (2020); Jogenfors et al. (2015); Dong & Teng (2010); Liu et al. (2020). Device-independent QKD protocols were discussed by the authors Ursin et al. (2007); Liu et al. (2022); Wang & Huberman (2022); Li et al. (2022); Nadlinger et al. (2022); Wen-Zhao et al. (2022).

Researchers are experimenting with the QKD via quantum networks to evolve point-to-point communication (Zhou et al., 2022; Molotkov, 2022; Nadlinger et al., 2022). The error rate has been increased with the presence of inbuilt noise in quantum states although entangled qubits are used for QKD. The error correction methods need to be applied along with the QKD protocols to reduce the error rate. It is difficult to apply error correction strategies on fragile entangled qubits. There are various quantum error correction (QEC) strategies like Shor's 9-qubit QEC (Shor, 1995), repetition code (Wootters & Zurek, 1982), Quantum BCH codes (Aly et al., 2007), Steane's QEC (Steane, 1996b), Stabilizer codes (Pan & Nguyen, 2016), LDPC codes (Zhou et al., 2022) and many more. It is not so easy to apply all these codes in QKD due to the higher error rates. It has been observed from the literature that the error rate in QKD increases with the noise in the quantum system. The communication efficiency and quantum key length are also affected by the noise while transmitting the quantum information.

From the extensive literature on various Quantum Error Correction methods, Entanglement Purification protocols and Quantum Cost Optimization models, the observed limitations and research gaps are outlined in the following section.

2.6 Research gaps

Quantum error correction plays an important role in quantum computation. Various error correction methods were proposed by the authors to detect and correct the quantum errors. After the extensive literature review on existing quantum error correction methods, we observed the following open issues and research gaps for further simplification.

- Most of the QEC codes are symmetric. Symmetric error correction codes are implemented by keeping in mind that the probability of getting bit and phase flip errors is the same. But in reality, the probability of getting phase errors is more compared to the bit flips. The development of an asymmetric error correction code is required to reduce phase errors.

- The entanglement plays an important role in QEC. Entangled pairs are used for secure data transmission. Still, weak entanglement leads to more errors.

- Most of the existing QEC codes are developed to detect and correct only bit-flip errors but not phase-flip or both.

- The noise in the channel will increase the Quantum Bit Error Rate (QBER) and reduce the quantum state's fidelity.

- Error correction codes like Repetition code, CWS Code and Decoupling transversal code work efficiently on 3 qubit systems. The performance of these codes will be degraded if the number of qubits is increased.

- The QEC codes with parameters [n,k,d] increases the quantum cost and depth with a higher value of n (i.e. with more number of qubits), which in turn increases the hardware requirements of the quantum system.

- Developed QEC architectures must be of low cost; otherwise, the hardware requirements and power consumption of the quantum system increases.

- Many existing QEC methods are implemented using higher-cost quantum gates. It increases the overall cost and also affects the performance of the quantum system.

2.7 Problem Statement

Based on the understanding of the gaps identified from the review of existing literature in the domain of Quantum Error Correction, the research problem is defined as follows:

"To design and develop an Enhanced Architecture for Asymmetric Quantum Syndrome Error Correction"

2.8 Objectives

Based on the outcome of the literature survey and defined problem statement, three objectives are defined as follows:

1. To design and develop an efficient Entanglement Purification method to distil the maximally entangled pair.
2. To design and develop an efficient Asymmetric Quantum Syndrome Error Correction in a multi-input Quantum system.
3. To design and develop a Quantum Cost Optimization model for the proposed Asymmetric Quantum Syndrome Error Correction.

2.9 Summary

In this chapter, we discussed in detail about Quantum computing and the significance of error correction methods in quantum systems. Also presented extensive literature on Quantum Error Correction, Entanglement Purification, Quantum Cost Optimization and Quantum Key Distribution protocols with their merits and demerits by considering current scenarios. The research gaps and challenging issues arised based on the literature are clearly listed along with the problem statement and research objectives. In the next chapter, we formally define the research problem addressed in this thesis. Also briefly discuss the proposed methodologies designed to address the observed research gaps. The details of these are presented in subsequent chapters of this thesis.

Chapter 3

Architecture for Asymmetric quantum Syndrome Error Correction

We have discussed the problems of the preset classical systems and a way towards the development of various Quantum architectures in the previous chapter. This chapter briefly discusses the architecture of Asymmetric Quantum Syndrome Error Correction required for secure quantum communication using the entangled qubits, encoding, error detection and correction and decoding operations along with the quantum system requirements from one system to another system. Also explains in detail the Quantum communication required for error detection and correction and the importance of the QKD in Quantum Communication.

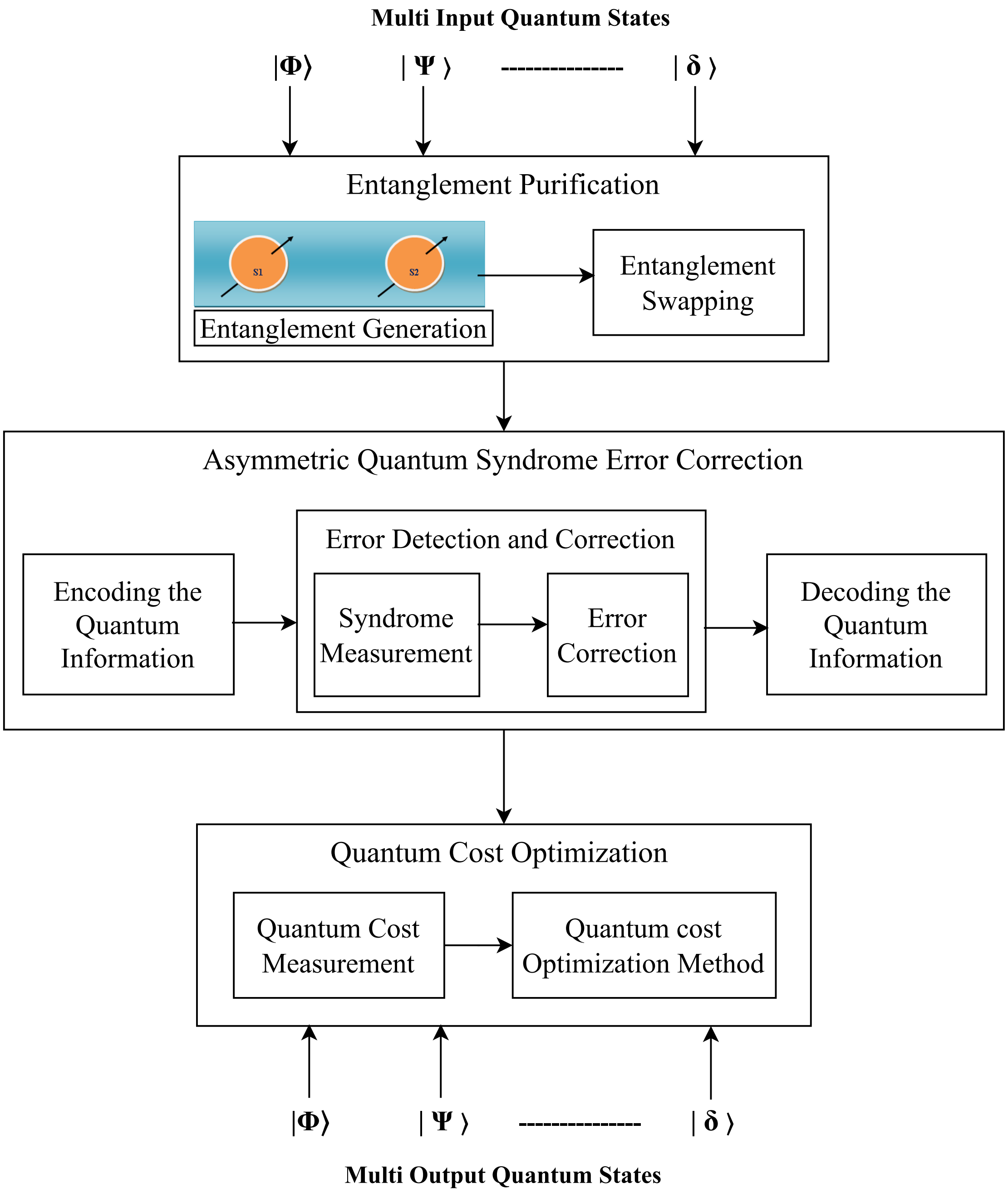
From the extensive literature review of the existing state-of-the-art methods to design quantum error correction strategies, it is observed that the implementation of asymmetric quantum error correction methods is crucial in current NISQ-level quantum systems to detect and correct both bit and phase flip errors. It was also observed that the effectiveness of Quantum error correction would be improved with the usage of entangled qubits while performing the error detection and correction in a quantum system. With this objective and with the aim of reconciling the observed gaps, the research work proposed in this thesis has been briefly explained with proposed research objectives in the following section.

3.1 Brief overview of Proposed Methodology

The overall architecture of the proposed Asymmetric Quantum syndrome error correction is depicted in Figure 3.1. The various contributions made towards the defined research objectives are indicated with respect to the individual thesis chapters in which they are discussed in more detail. Here, a brief outline of the overall research work presented in this thesis is discussed.

3.1.1 Entanglement Purification

Entanglement is an essential property of Quantum particles, which plays an important role in developing Quantum error correction methods. However, from the existing lit-


Multi Input Quantum States
|Φ⟩
|Ψ⟩

|δ⟩
Entanglement Purification
S1
S2
Entanglement Generation
Entanglement Swapping
Asymmetric Quantum Syndrome Error Correction
Encoding the Quantum Information
Error Detection and Correction
Syndrome Measurement
Error Correction
Decoding the Quantum Information
Quantum Cost Optimization
Quantum Cost Measurement
Quantum cost Optimization Method
|Φ⟩
|Ψ⟩

|δ⟩
Multi Output Quantum States

Figure 3.1: Architecture for Asymmetric Quantum Syndrome Error Correction

erature, it has been observed that the quantum error correction using entangled qubits overcomes the drawbacks of symmetric quantum error correction. When we use entangled qubits to develop an error correction method, we need to consider a maximally entangled pair. Otherwise, it leads to more errors and data loss. To reduce these errors, we propose a novel and efficient entanglement purification method to distil the maximally entangled pairs from weak ones. The generic workflow of the proposed entanglement purification method is depicted in Figure 3.2.

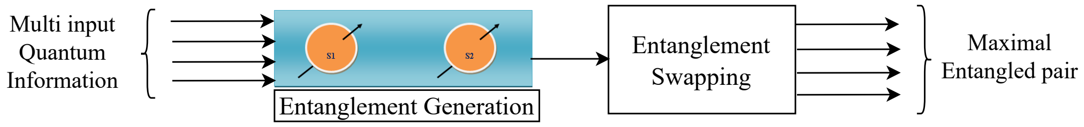


Figure 3.2: Workflow of Entanglement Purification

As shown in Figure 3.2, the research contributions to develop an entanglement purification method include Entanglement generation and Entanglement swapping. To generate the entanglement, various quantum gates will be applied on multi-input quantum information. After generating the entanglement, entanglement swapping will be performed on generated entangled pairs to distil the maximally entangled pair. A detailed discussion of the proposed entanglement purification method is given in Chapter 4.

3.1.2 Asymmetric Quantum Syndrome Error Correction

Quantum error correction plays an important role in current Noisy Intermediate Scale level Quantum systems. The error rates in these quantum systems are very high due to the inbuilt noise, which in turn leads to errors. Error correction methods must be implemented to protect the information and detect & correct errors. It has been observed from the literature that there is a huge requirement for asymmetric quantum error correction. We observed in the literature most of the existing error correction methods are symmetric and can detect either bit-flip or phase-flip errors. To address these problems an efficient asymmetric quantum error correction method is required which is proposed. A methodology for Asymmetric Quantum Syndrome Error Correction is depicted in Figure 3.3.

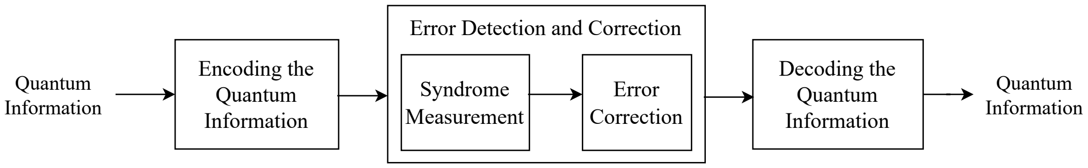


Figure 3.3: Methodology for Asymmetric Quantum Syndrome Error Correction

As shown in Figure 3.3, the research contributions to develop asymmetric quantum error correction includes Encoding the logical quantum state into multiple physical quantum states, Error detection and Correction using syndrome measurement, and finally decoding the quantum information by performing various quantum operations. A detailed discussion of these contributions is presented in Chapter 5.

3.1.3 Quantum Cost Optimization

Cost is one of the major parameters that need to be considered while developing an efficient algorithm or architecture to solve a specific problem. Similarly in Quantum computation, quantum cost optimization plays an important role in optimizing the architecture in terms of quantum gates and operations. After implementing the error correction method, it is important to optimize the cost to reduce the hardware requirements. It has been observed from the literature that the quantum cost of the existing state-of-the-art methods is high. This proves that there is enormous scope to develop an efficient algorithm to optimize the quantum cost. To address this, an efficient method for Quantum cost optimization is required. A methodology for Quantum cost optimization is depicted in Figure 3.4.

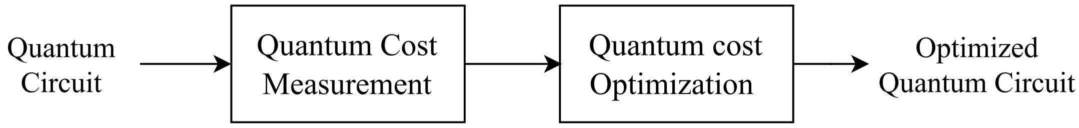


Figure 3.4: Methodology for Quantum Cost Optimization

As shown in Figure 3.4, the research contributions to develop a quantum cost optimization algorithm includes Quantum cost measurement and Quantum cost optimization. To perform these operations, the input will be considered as a quantum circuit and the outcome will be an optimized quantum circuit. The detailed elucidation on quantum cost optimization is presented in Chapter 6.

3.1.4 Quantum Key Distribution

Entanglement purification and Quantum error correction play a prominent role in various applications like Quantum key distribution, Secure communication, Quantum repeaters, etc. To prove the efficiency of the proposed methods, the Quantum key distribution protocol is developed using the Asymmetric Quantum Syndrome Error Correction. The workflow of the proposed Quantum key distribution with an error correction mechanism is depicted in Figure 3.5. The detailed discussion on the design and development of Quantum key distribution protocol is presented in Chapter 7.

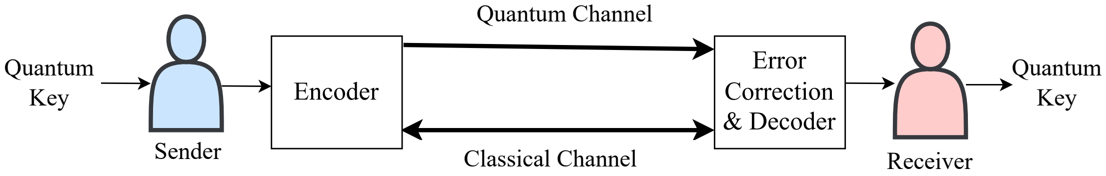


Figure 3.5: Process of Quantum Key Distribution

3.2 Research Contributions

This thesis presents a framework for detecting and correcting quantum errors using an asymmetric quantum error correction method with the advantage of entanglement. The objectives are to design efficient approaches for entanglement purification, Quantum error correction, and Quantum cost optimization using appropriate quantum operations. With regard to the outcomes gleaned from the literature review and the scope of work presented, the major contributions of our research work presented in the subsequent chapters of this thesis are as follows:

- An empirical study on the various quantum gates and the implementation of an efficient approach to generate entanglement from the quantum information.

- Implementation of Entanglement swapping by performing quantum operations using quantum gates to purify the entanglement.

- Developing an efficient encoding method by performing phase operations to strengthen the original quantum information.

- Development of quantum error detection and correction with syndrome measurement using the hamming bound.

- Perform decode operation to decode the encoded information into originally transmitted information.

- Development of quantum cost optimization algorithm to optimize the overall cost of the proposed error correction method.

- Development of Quantum key distribution protocol using Quantum error correction to analyze the efficiency of the proposed error correction method.

3.3 Summary

In this chapter, we have presented the proposed methodology for Asymmetric Quantum Syndrome Error Correction. Discussed briefly about the research objectives with the proposed workflow. The significant contributions of the research work are outlined. The detailed discussion of each objective along with the proposed methodology are presented in the subsequent chapters.

Chapter 4

Entanglement Purification using Entanglement Swapping

In the previous chapter, a brief overview of the Asymmetric Quantum Syndrome Error Correction mechanism and required methodology has been presented. This chapter explains about Entanglement Purification using Entanglement Swapping which is required for efficient Quantum communication. The main goal of this chapter is to discuss in detail about the development of Entanglement Purification along with Entanglement Swapping and compare the performance analysis with the currently available methods.

4.1 Importance of Entanglement Purification

Entanglement is a principal resource for Quantum Information Process. It plays a key role in applications like Quantum Communication, Teleportation, Quantum Key Distribution, Quantum Repeaters and etc. Strong entangled pairs are required for efficient data transmission in these applications. System impurities during the data transportation weaken the entanglement and reduce the fidelity of the entangled pair (Pan et al., 2001). Therefore the necessity of entanglement purification techniques is very high to distil strong entangled pairs from weakly entangled ones. Moreover, entanglement plays an important role in quantum error correction because it significantly increases the quality of the operations between qubits. Since the error rate in quantum communication is very high due to the noise and decoherence (Shnirman et al., 2002). The entangled qubits give an efficient result in protecting the qubit and performing error correction. The entanglement between qubits must be robust; otherwise, it leads to errors. Entanglement purification methods need to be implemented to solve the issue. To develop the Entanglement Purification technique, two major steps need to be performed. These are entanglement generation and entanglement Swapping.

4.2 Entanglement Generation

As per the Information theory, Shannon's entropy is used to generate and measure the entanglement. Shannon Entropy represents the probability distribution of pure events

$d_1, d_2, d_3, ---, d_n$ in a Hilbert space $\mathcal{H}$. It is defined as follows.

$$\mathcal{H}(d_1, d_2, ---, d_n) = -\sum_k d_k log_2 d_k \tag{4.1}$$

When the operations are performed on pure quantum states, those will be converted to the mixed states (let us say ρ) due to the external interaction and noise. In such cases, the probability distribution of Shannon's entropy is modified as follows.

$$V(\rho) = -Tr(\rho log_2 \rho) \tag{4.2}$$

The above equation is further simplified by calculating the eigenvalues of ρ. Let us say $\Lambda_1, \Lambda_2, ----, \Lambda_n$ in a Hilbert space $\mathcal{H}$ is as follows.

$$V(\rho) = -\sum_k \Lambda_k log_2 \Lambda_k \tag{4.3}$$

In Shannon's entropy, Eigenvalues are used to specify the limit of information to be transmitted over the communication channel. Here eigenvalues are also used to calculate the entanglement between quantum states and to retrieve the maximum value by performing uniform probability distribution. Thus to measure the entanglement, the equation (4.3) will be modified as follows.

$$\text{Entanglement measurement} = \tfrac{1}{\sqrt{2}}(|a\rangle^{\otimes N} + |b\rangle^{\otimes N}) \tag{4.4}$$

Where $|a\rangle$ and $|b\rangle$ are the quantum states and N is the total number of quantum states.

Before transmitting the data using ebits(entangled qubits), it is necessary to develop a maximally entangled channel to generate maximal ebits. The noise and decoherence present in the channel leads to weak entanglement and degrades communication efficiency. Thus the implementation of entanglement purification (EP) methods is inevitable. Usually, bell states are used to represent ebits. For example **a, b** are two parties and maximally entangled, then the total possible bell states to represent ebits are four. The equations to measure bell states can be written by simplifying the equation (4.4) as follows.

$$|\psi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|0_a\rangle|0_b\rangle + |1_a\rangle|1_b\rangle) \tag{4.5}$$

$$|\psi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0_a\rangle|0_b\rangle - |1_a\rangle|1_b\rangle) \tag{4.6}$$

$$|\phi^+\rangle_{ab} = \frac{1}{\sqrt{2}}(|0_a\rangle|1_b\rangle + |1_a\rangle|0_b\rangle) \tag{4.7}$$

$$|\phi^-\rangle_{ab} = \frac{1}{\sqrt{2}}(|0_a\rangle|1_b\rangle - |1_a\rangle|0_b\rangle) \tag{4.8}$$

Here $|0\rangle$ and $|1\rangle$ are the Quantum States. Quantum states are represented with vectors. A tensor operation will be performed on these vectors to represent the entangled states. Tensor operations are used to represent the vectors with higher dimensions and to perform operations on them. Let us assume a 4-qubit quantum system in which first and second qubits, third and fourth qubits are entangled in $|\psi^-\rangle$ bell state. Then the resulting entangled pair can be represented by performing a tensor operation on vectors as follows.

$$\begin{aligned}
|\psi\rangle_{1234} &= |\psi^-\rangle|\psi^-\rangle \\
&= \frac{1}{\sqrt{2}}(|0_a\rangle|0_b\rangle - |1_a\rangle|1_b\rangle) \otimes \frac{1}{\sqrt{2}}(|0_a\rangle|0_b\rangle - |1_a\rangle|1_b\rangle) \\
&= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \\
&= \frac{1}{2}\begin{matrix}(1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1)^T\end{matrix}
\end{aligned} \tag{4.9}$$

In the above equation (4.9), the tensor operation is performed on two vectors of size 4x1, 4x1. After performing the operation the resulted vector is of size 16x1. In quantum operations, whenever the operations are performed on more number of qubits then the vector size of the resulted state will be increased. Similarly, we can also use Bell states as in equations (4.5), (4.7) and (4.8) based on the requirement. In a quantum system, entanglement is generated using Hadamard and Controlled-NOT (CNOT) gates. As discussed in section 1.3.1, the Hadamard gate is a single input and single output gate. It is mainly used to represent the superposition of a qubit. CNOT gate is a two-input and two-output gate. The CNOT gate contains 2 inputs called Control and Target inputs and 2 outputs called Control and Target outputs. If the control input is $|0\rangle$ then the Target output will be the same as the target input but if the control input is $|1\rangle$ then the target output will be the complement of the target input as discussed in section 1.3.2. The matrix representation of the CNOT gate is as follows.

$$\text{CNOT Gate} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CNOT operations can also be performed using Hadamard Basis. For an example, consider a two-stage quantum system with states $|0\rangle$, $|1\rangle$. The output of a Hadamard gate for any input either $|0\rangle$ or $|1\rangle$ will be the superposition of both. It can also be represented for both +ve and -ve phases, which we call as Hadamard basis and can be represented as $H = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$.

4.2.1 Entanglement generation using 2-Qubits (Bell pair $|\phi^+\rangle_{AB}$)

In this experiment, we considered the bell pair $|\phi^+\rangle_{AB}$ to generate the entanglement between 2 qubits. Initially, two inputs $|0\rangle$, $|1\rangle$ are considered to generate $|\phi^+\rangle_{01}$ using Hadamard and CNOT gates. The detailed circuit diagram of $|\phi^+\rangle_{01}$ is depicted in following Figure 4.1.

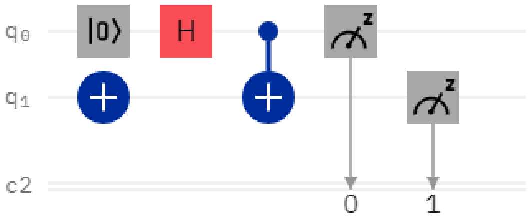


Figure 4.1: Quantum Circuit diagram for 2-Qubit Entanglement. q_0 and q_1 are input variables and c2 is an output variable. This circuit illustrates the Bell state $|\phi^+\rangle$ with inputs $|0\rangle$ and $|1\rangle$.

As per the Hadamard operation, for input $|0\rangle$ the resulted outcome will be $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. If we try to measure the outcome of Hadamard gate, it will be lost into either state $|0\rangle$ or $|1\rangle$ based on the highest probability. For example, if the output of the Hadamard gate is $|0\rangle$, then the target output of the CNOT gate is the same as input q1 that is state $|1\rangle$. Then the final outcome of the circuit will be $|01\rangle$. Otherwise, if the Hadamard gate output is $|1\rangle$, then the final output of the circuit after the CNOT operation will be $|10\rangle$.

The mathematical equation for Hadamard and CNOT operations is as follows.

$$
\begin{aligned}
c2 &= CNOT\left[H(|0\rangle), |1\rangle\right] \\
&= CNOT\left[\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, |1\rangle\right] \\
&= \left[|01\rangle, |10\rangle\right]
\end{aligned}
\tag{4.10}
$$

As simplified in equation (4.10), the estimated result of the 2-Qubit entanglement circuit should result in states $|01\rangle$ and $|10\rangle$ only. But after running the circuit (Figure 4.1) in IBM Quantum Computer using the Qiskit tool (Qiskit (Qiskit, 2019) is an open-source platform developed by IBM to perform operations with their Quantum Computer), the retrieved results are shown in the form of a probability measurement chart as in Figure 4.2.

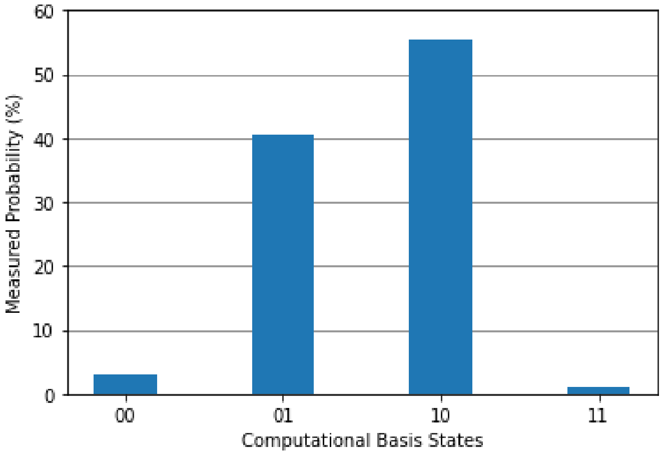


Figure 4.2: Probability Measurement Chart of 2-Qubit Entanglement Circuit after running in the IBM Quantum System.

The expected outcome of the circuit (Figure 4.1) is $|01\rangle$, $|10\rangle$ states with the probability of 50%. From Figure 4.2, it is observed that the generated entanglement is not maximal. i.e the probability of resulting states $|01\rangle$, $|10\rangle$ for $|\phi^{+}\rangle$ are modified. Along with the expected output states, we also retrieved states $|00\rangle$ and $|11\rangle$ with probabilities 3% and 1% respectively. The outcome is transpiled due to the occurrence of phase or bit shifts while running the circuit in Quantum Computer due to the noise. The detailed transpiled circuit with impurities is represented in Figure 4.3.

In Figure 4.3, RZ represents the rotation of the qubit over the Z-axis. The phase shift in a qubit, and $\sqrt{X}$ represents the rotation over the X-axis, i.e., the bit shift. These

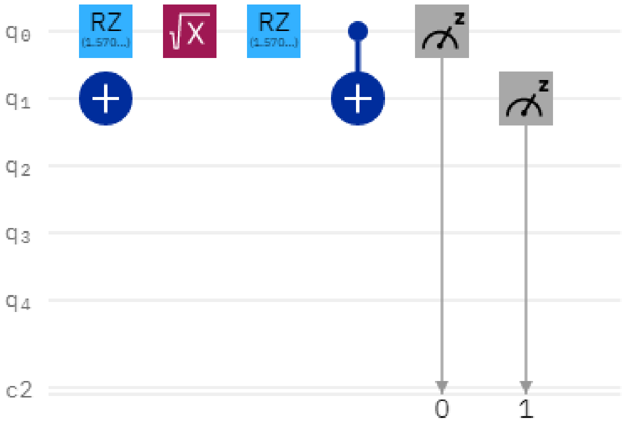


Figure 4.3: Transpiled Circuit diagram of 2-Qubit Entanglement.

are generated due to the noise or error associated with the quantum gates in the Quantum System. To observe the results of the two entangled pairs, the experiments are performed with 4-qubit entanglement using two entangled pairs.

4.2.2 Entanglement generation using 4-Qubits (Bell pair $|\phi^+\rangle_{AB}$)

To implement 4-qubit entanglement, two entangled pairs are required with Hadamard and CNOT operations. The circuit representation of 4-qubit Entanglement using Hadamard and CNOT gates is depicted in Figure 4.4.

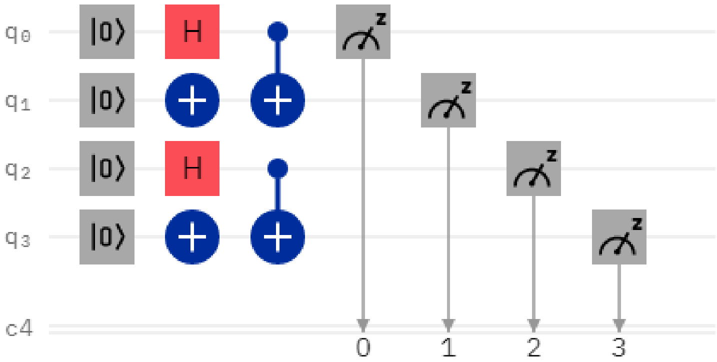


Figure 4.4: Quantum Circuit diagram for 4-Qubit Entanglement. Here q_0, q_1, q_2, q_3 represents the inputs and c4 represents the output

The mathematical calculation of the 4-qubit entanglement with bell state $|\phi^+\rangle$ is as follows.

$$
\begin{aligned}
c4 &= CNOT\left[H(|q0\rangle), |q1\rangle\right], CNOT\left[H(|q2\rangle), |q3\rangle\right] \\
&= CNOT\left[H(|0\rangle), |1\rangle\right], CNOT\left[H(|0\rangle), |1\rangle\right] \\
&= CNOT\left[\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, |1\rangle\right], CNOT\left[\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, |1\rangle\right] \\
&= [|01\rangle, |10\rangle], [|01\rangle, |10\rangle] \\
&= [|0101\rangle, |0110\rangle, |1001\rangle, |1010\rangle]
\end{aligned} \tag{4.11}
$$

As in equation (4.11), the output of a 4-qubit entanglement circuit as in Figure 4.4 should contain only the states $|0101\rangle$, $|0110\rangle$, $|1001\rangle$ and $|1010\rangle$ with equal probabilities. After running the circuit on Quantum System, the results have deviated as shown in Figure 4.5. Its transpiled diagram with system impurities is depicted in Figure 4.6.

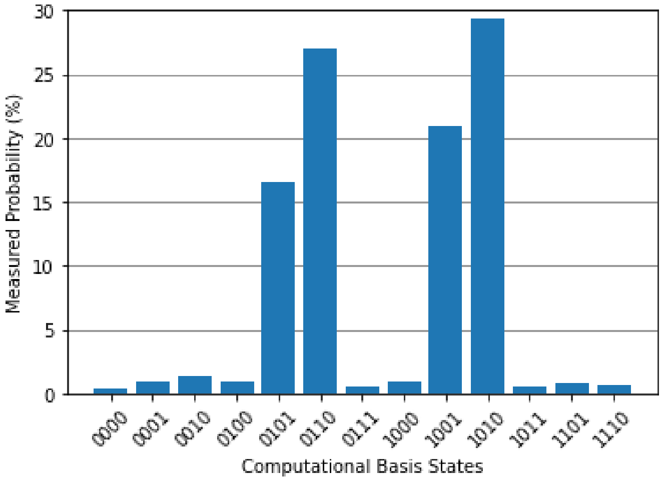


Figure 4.5: Probability Measurement Chart of 4-Qubit Entanglement after running in Quantum system.

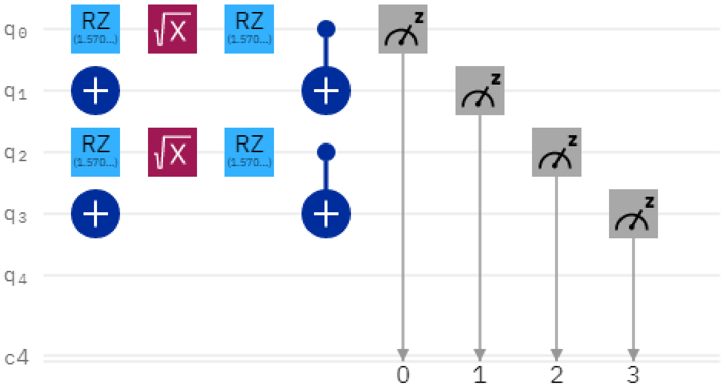


Figure 4.6: Transpiled Circuit diagram of 4-Qubit Entanglement.

From Figures 4.5 and 4.6, it is observed that the output of 4-qubit entanglement after running it in a Quantum computer is different when compared to the theoretical calculations. This is because of the inbuilt noise of the quantum system which in turn leads to imperfect or weak entanglement. As shown in Figure 4.5, the output contains the extra states $|0001\rangle$, $|0010\rangle$, $|0100\rangle$, $|0111\rangle$, $|1000\rangle$, $|1011\rangle$, $|1101\rangle$ and $|1110\rangle$ along with the expected output states $|0101\rangle$, $|0110\rangle$, $|1001\rangle$ and $|1010\rangle$. The Transpiled circuit diagram of phase and bit shifts along with the X, Y, and Z-axis is shown in Figure 4.6. The bit and phase shifts result in weak entanglement. Hence it is necessary to apply entanglement purification techniques to reduce the errors and to generate maximal entanglement. The steps to measure the probability, error rate and fidelity of the entire system are discussed in the following section.

4.3 System Probability, Error rate and Fidelity Measurement

The probability measurement of the entire system will be used to calculate the error rate. In the current era of quantum systems, the experimental results and actual results may not be the same. Fidelity measurement is used to calculate the fidelity of the current state to the target state.

4.3.1 Probability and Error rate Measurement

To perform entanglement purification, it is essential to calculate the probability of the entire system along with the error rate. The error (Phase or Bit) rate must be reduced in order to maximize the entanglement between qubits. The steps to measure the system probability with noise are as follows.

The system probability ρ can be measured using the following equation.

$$\rho = \sum_{k} P_k |\phi_k\rangle\langle\phi_k|$$

Where $|\phi\rangle$ represents the quantum state, k is the number of stages, and P is the probability of becoming state $|\phi\rangle$.

Let us consider k=2, i.e., a 2-stage quantum system. The final probability along with probability P_i of the entire system with noisy or error states is calculated by using the following equation.

$$\rho = P_i|\phi_{ab}\rangle\langle\phi_{ab}| + (1 - P_i)|ab\rangle\langle ab|$$

Where P_i is the probability of noise state, and $1 - P_i$ is the probability of the entire system. After measuring the probability of the system, it is also important to calculate the fidelity of the system.

4.3.2 Fidelity Measurement

At present, the quantum systems which we are using to perform experiments are in the Noisy Intermediate Scale Quantum (NISQ) Level. The result of a quantum architecture executed on a NISQ level quantum system will never be 100% due to the inbuilt noise. There is a difference between actual and retrieved outputs. Fidelity measurement is used to measure the closeness between the expected and retrieved outcomes. Fidelity measurement is also used to measure the efficiency of a quantum architecture after running it on a Quantum computer (Ouyang & Lai, 2022).

For example, if we want to transmit the information $|\phi\rangle$ from one end to another. But after running the architecture in the quantum system, the retrieved result is $|\rho\rangle$. The fidelity of the resulting quantum state is measured using the following equation.

$$F = \langle\phi|\rho|\phi\rangle \tag{4.12}$$

Where ρ represents the density matrix of the state we received. It can be measured as follows.

$$\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i| \tag{4.13}$$

Here p_i is the probability of the state $|\phi_i\rangle$. The final value of the fidelity lies between 0 & 1 and will be converted into percentages by considering maximum achievable fidelity which is equal to 1 as 100%.

One possible way to reduce the noise and generate the maximally entangled pair is entanglement swapping. Entanglement purification can be realized by using entanglement swapping.

4.4 Entanglement Swapping

Entanglement Swapping plays a vital role in Entanglement purification and long-distance communication. Due to the decoherence, it is difficult to transmit the maximally entangled qubits to longer distances. It leads to the decay in Quantum information transmission. To overcome this problem, entanglement swapping can be performed. Swapping operation divides the longer distances into shorter distances by maintaining the maximal entanglement between entangled qubits. Swapping is not only a principal resource for entanglement purification but also plays a vital role in various applications like quantum repeaters, quantum teleportation, etc. Entanglement purification is achieved for discrete and continuous variables using single-stage photons. But multistage swapping provides higher quantum state protection over noise and errors. The process of entanglement swapping is realized in the following Figure 4.7.

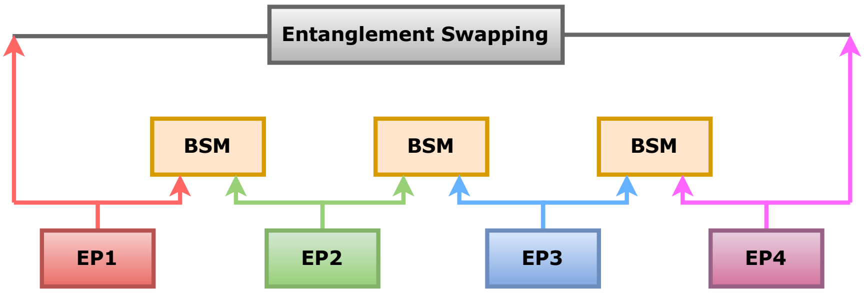


Figure 4.7: Representation of 4-stage Entanglement Swapping with Bell State Measurement (BSM). Here total 4 Entangled Pairs(EP's) and 3-BSM's are used to perform Entanglement Swapping.

Figure 4.7 shows the entanglement swapping procedure. To explain clearly about the process we have considered 4-entangled pairs. The primary goal of entanglement swapping is to distil the maximally entangled pairs. In order to do this, bell state measurements (BSM) will be performed. Swapping is used to transfer the entanglement for longer distances by combining the maximally entangled qubit of the first entangled pair with the maximally entangled qubit of the last entangled pair. The entanglement swapping process can be explained clearly with the help of Figure 4.7. In Figure 4.7, EP1 represents the entanglement between qubits 1 and 2. EP2 represents the entanglement between qubits 3 and 4, EP3 represents the entanglement between qubits 5 and 6, and EP4 represents the entanglement between qubits 7,8. BSM represents the Bell-State Measurement. BSM measures the maximal and weaker entangled qubits in an entangled pair. Based on the outcome of the BSM, the maximally entangled qubits are connected by swapping the entanglement between weaker entangled qubits. For example, if the entangled qubits 2, and 3 of EP1, and EP2 are weak, then the entanglement will be swapped between qubits 1 and 4 and qubits 2, and 3. Similarly, the entanglement between qubits 2 and 3, 4 and 5, 6 and 7 of different EP's are swapped. Finally, the entanglement will be generated between qubits 1 and 8 by performing swapping operation. The mathematical representation of the entanglement swapping is given below.

$$|\phi\rangle = \Sigma_n \sqrt{\Lambda_n} |P_n\rangle \oplus |Q_n\rangle \tag{4.14}$$

Here $\sqrt{\Lambda_n}$ is the Schmidt coefficient. $\sqrt{\Lambda_n}$ is used to measure the entanglement. Its value must be $\sqrt{\Lambda_n} \geq 0$. It is calculated by performing the inner product on the quantum states. For example, if a state $|\delta\rangle$ contains only one Schmidt coefficient then it is called as a separable state. If it contains more than one Schmidt coefficient, then it is known as an entangled state. If all the Schmidt coefficients of a state are non-zero's, then it is represented as a maximally entangled state.

Let us consider entanglement swapping with four entangled pairs as in Figure 4.7 with bell state $|\phi^+\rangle$. Then the equation (4.14) is modified as follows.

$$\begin{aligned} |\phi^+\rangle_{12345678} &= |\phi^+\rangle_{12} + |\phi^+\rangle_{34} + |\phi^+\rangle_{56} + |\phi^+\rangle_{78} \\ &= ((|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2)/\sqrt{2}) \\ &+ ((|0\rangle_3 |1\rangle_4 + |1\rangle_3 |0\rangle_4)/\sqrt{2}) \\ &+ ((|0\rangle_5 |1\rangle_6 + |1\rangle_5 |0\rangle_6)/\sqrt{2}) \\ &+ ((|0\rangle_7 |1\rangle_8 + |1\rangle_7 |0\rangle_8)/\sqrt{2}) \end{aligned} \tag{4.15}$$

After performing the entanglement swapping between 4 entangled pairs(EP's), the equation 4.15 is further simplified as follows.

$$
\begin{aligned}
|\phi^{+}\rangle_{12345678} &= |\phi^{+}\rangle_{14} + |\phi^{+}\rangle_{23} + |\phi^{+}\rangle_{58} + |\phi^{+}\rangle_{67} \\
&= ((|0\rangle_{1}|1\rangle_{4} + |1\rangle_{1}|0\rangle_{4})/\sqrt{2}) \\
&+ ((|0\rangle_{2}|1\rangle_{3} + |1\rangle_{2}|0\rangle_{3})/\sqrt{2}) \\
&+ ((|0\rangle_{5}|1\rangle_{8} + |1\rangle_{5}|0\rangle_{8})/\sqrt{2}) \\
&+ ((|0\rangle_{6}|1\rangle_{7} + |1\rangle_{6}|0\rangle_{7})/\sqrt{2})
\end{aligned}
\tag{4.16}
$$

The equation 4.16 is further simplified as follows by removing the weaker entangled qubits.

$$
\begin{aligned}
|\phi^{+}\rangle_{12345678} &= |\phi^{+}\rangle_{14} + |\phi^{+}\rangle_{58} \\
&= ((|0\rangle_{1}|1\rangle_{4} + |1\rangle_{1}|0\rangle_{4})/\sqrt{2}) \\
&+ ((|0\rangle_{5}|1\rangle_{8} + |1\rangle_{5}|0\rangle_{8})/\sqrt{2})
\end{aligned}
\tag{4.17}
$$

The equation of the final maximal entangled pair of qubits 1 and 8 after performing the entanglement swapping is as follows.

$$
|\phi^{+}\rangle_{18} = (|0\rangle_{1}|1\rangle_{8} + |1\rangle_{1}|0\rangle_{8})/\sqrt{2} \tag{4.18}
$$

With the advantage of entanglement swapping, we proposed an entanglement purification method to distil the maximal entanglement from the weaker one. The detailed algorithm for the entanglement purification method with Entanglement generation and Entanglement swapping is represented in Algorithm 4.1.

Algorithm 4.1 An algorithm for Entanglement Purification

```
Input:  Quantum States
Output: Maximally Entangled Pair
Initialize Quantum Register q and Classical Register c with size 4
Initialize the Number of qubits n as 4
$q[1] \leftarrow X$
$q[3] \leftarrow X$
$q[0]$ & $q[1] \leftarrow$ CNOT
$q[0] \leftarrow H$
$q[0]$ & $q[3] \leftarrow$ CNOT
```

```
$q[3] \leftarrow H$
$q[0]$ & $q[1] \leftarrow$ CNOT
$q[0] \leftarrow H$
$q[2]$ & $q[3] \leftarrow$ CNOT
$q[2] \leftarrow H$                    ▷ Entanglement Generation & Bell State Measurement
$q[0]$ & $q[3] \leftarrow$ CNOT
$q[3]$ & $q[0] \leftarrow$ CNOT
$q[0]$ & $q[3] \leftarrow$CNOT
$q[2] \leftarrow H$
$q[1]$ & $q[2] \leftarrow$ CNOT
$q[2]$ & $q[1] \leftarrow$ CNOT
$q[1]$ & $q[2] \leftarrow$ CNOT
for i=0 to n-1 do
    $c[i] \leftarrow q[i]$
end for
for i=0 to n-1 do
    Measure c[i]                       ▷ Entanglement Swapping and Purification
end for
```

As written in Algorithm 4.1, the entanglement generation and swapping steps are performed to purify the entanglement. We considered the input combination as $|1010\rangle$ for the experiment. CNOT and Hadamard gates are used to generate the entanglement between pairs $|q_0\rangle, |q_1\rangle$ & $|q_2\rangle, |q_3\rangle$. Bell state measurement will be performed by measuring the probabilities of Entangled pairs after generating the entanglement. Based on these values, entanglement swapping is performed to swap the entanglement between strongly entangled qubits by performing CNOT gate operations. CNOT gate swaps the entanglement between pairs $|q_0\rangle$ & $|q_3\rangle$ by separating the quantum states $|q_1\rangle$ & $|q_2\rangle$ from its entangled pairs as described in equation (4.15) for the input states $|0\rangle, |1\rangle, |0\rangle, |1\rangle$. The CNOT operations between $|0\rangle|1\rangle$ with Hadamard gate produce the output as the first entangled pair i.e. $|1\rangle|0\rangle$. The CNOT and Hadamard operations on the input states $|0\rangle|1\rangle$ produce the second entangled pair i.e. $|1\rangle|0\rangle$. Thus the output of the CNOT gate for input states $|1\rangle|0\rangle$ can be represented in the form of a density matrix which is given below.

$$|0\rangle|1\rangle \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

After that Hadamard operation will be performed on the outcome of the CNOT gate.

After performing the operation, the density matrix is modified as follows.

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix}$$

The final result of CNOT and Hadamard operations on the input states $|1\rangle|0\rangle$ can be represented as $|01\rangle \mapsto (|01\rangle + |10\rangle)/\sqrt{2}$.

Similarly, the CNOT and Hadamard operations will be performed on $|q_2\rangle, |q_3\rangle$. The output after the first part is $|1010\rangle$. The remaining algorithm in the second part swaps the entanglement between $|q_0\rangle$ & $|q_3\rangle$ and $|q_1\rangle$ & $|q_2\rangle$. The CNOT operation on states $|q_0\rangle, |q_3\rangle$ can be represented as $|q_0\rangle, |q_3\rangle$ = $|10\rangle$ CNOT $|10\rangle$. The outcome of this operation will be given to the Hadamard gates which are applied on $|q_0\rangle$ and $|q_3\rangle$. These operations swap and strengthen the entanglement between the first and last qubits by increasing the fidelity. The entire process of entanglement purification is developed and executed on a real Quantum system. The detailed result analysis of the proposed method along with the experimental setup are described in the following section.

4.5 Experimental Setup

The classical and Quantum systems are used for performing the experiments. The configuration details of the Classical system are given below.

- Processor: Intel core I3
- RAM: 4GB
- Operating System: Windows 7 Ultimate

The proposed Entanglement purification algorithm is implemented on IBM Quantum System using the Qiskit tool. The configuration details of the IBM quantum system are as follows.

- System Name: ibmq_manila
- Operating System: Darwin

- Tool used: Qiskit tool
- Simulator: ibmq_qasm_simulator
- Processor type: Falcon r5.11L

4.6 Discussion and Result Analysis

4.6.1 Discussion

After running the proposed algorithm (as in Algorithm 4.1) in the Quantum system, the retrieved results before and after entanglement swapping are depicted in Figure 4.8 & 4.9.

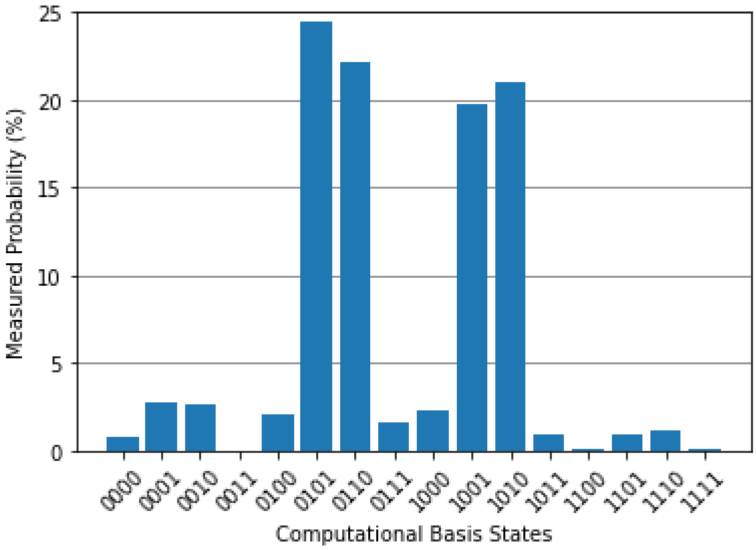


Figure 4.8: Quantum results for 4-Qubit Entanglement generation.

From Figures 4.8 and 4.9, we observed that there is an enormous difference between entangled qubits with and without swapping. Figure 4.8 represents the entanglement generation between two pairs using Hadamard and CNOT operations. The probability of resulting entangled pairs is very less. The probabilities of the 2nd and 3rd entangled qubits are less compared to the 1st and 4th entangled qubits. To improve the probability and generate a maximally entangled pair, entanglement swapping has been performed between qubits 1st, 4th and 2nd, 3rd. The results after swapping are depicted in Figure 4.9 where it is clearly observed that there is an improvement in entangled pair probability. The comparison between the measured probabilities of results depicted in Figures 4.8 & 4.9 is demonstrated in Figure 4.10.

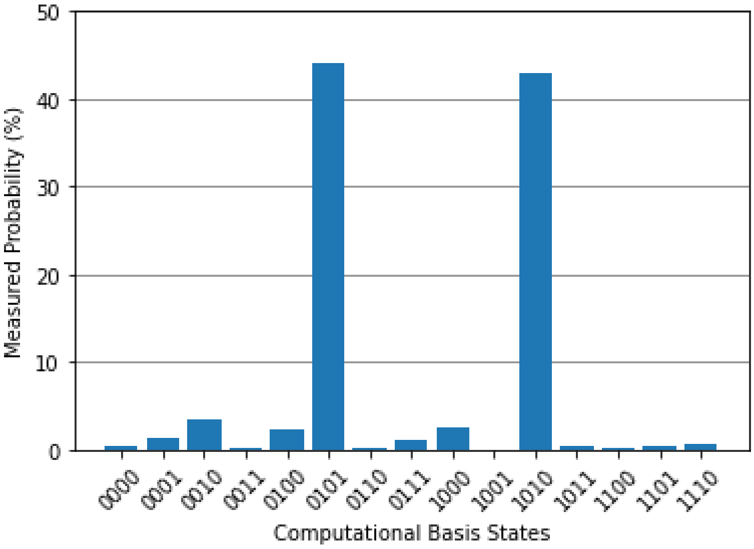


Figure 4.9: Quantum results for 4-Qubit Entanglement purification after swapping.

For the experiment, we have considered two entangled pairs with states $|B_2A_2B_1A_1\rangle = |1010\rangle$ as input states with bell state representation of $|\phi^+\rangle$. From Figure 4.9, it is observed that the entanglement between the pairs A_1, B_1 & A_2, B_2 has been swapped and resulted in a maximally entangled pair A_1, B_2. Whereas the entanglement between pair A_2, B_1 is weakly entangled. It can also be represented using the Bloch sphere. Bloch sphere represents the exact position of the quantum state in Hilbert space with X, Y, and Z axis. The Bloch sphere representation of the resulted maximally entangled pair is depicted in Figure 4.11.

The Bloch sphere represents the entanglement between quantum states in a graphical way. From Figure 4.11, it is clear that the first and last quantum states are entangled. Along with these, we measured the entanglement between the first and last qubits ($|q_0q_3\rangle$) and also the second and third qubits ($|q_1q_2\rangle$). The probability measurement of the entangled pairs $|q_0q_3\rangle$, $|q_1q_2\rangle$ are represented in Figure 4.12 & 4.13.

Figures 4.12, 4.13 shows the entanglement between pairs $|q_0\rangle$ & $|q_3\rangle$, $|q_1\rangle$ & $|q_2\rangle$. It is observed that the pair $|q_0\rangle$ & $|q_3\rangle$ is maximally entangled compared to the $|q_1\rangle$ & $|q_2\rangle$ pair. The fidelity measurement of the entangled pairs $|q_0\rangle$ & $|q_3\rangle$, $|q_1\rangle$ & $|q_2\rangle$ using the equation (4.12) is equal to 0.871, 0.772. Most of the existing methods have experimented on Simulators. To analyze the results of proposed and existing methods, we developed and executed the proposed method on a Quantum simulator. The observed results of entangled pairs are illustrated in Figure 4.14 & 4.15.

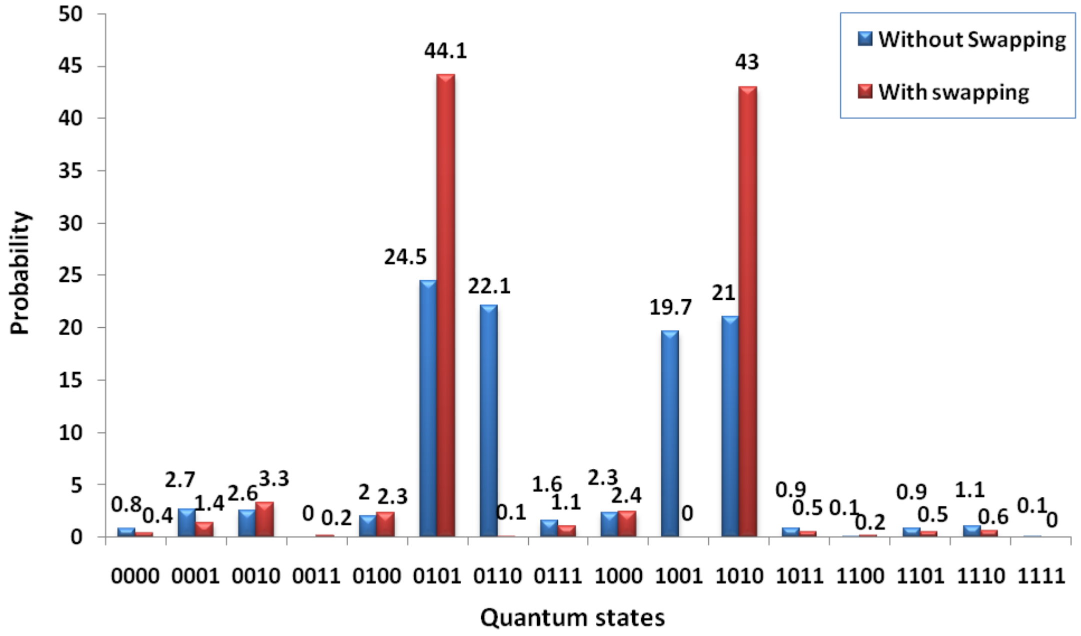


Figure 4.10: Probability comparisons of Figures 4.8, 4.9

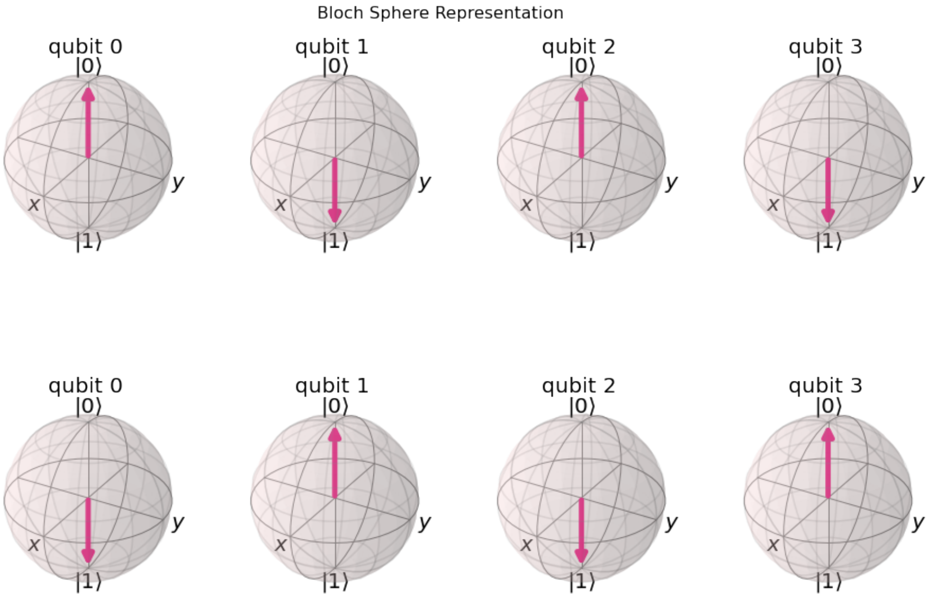


Figure 4.11: Bloch sphere representation of 4-Qubit Entanglement purification with swapping.

Figures 4.14 and 4.15 shows the Quantum simulator results for the entanglement between pairs $|q_0\rangle$ & $|q_3\rangle$, $|q_1\rangle$ & $|q_2\rangle$. From the results, it is observed that the pair $|q_0\rangle$ & $|q_3\rangle$ is maximally entangled compared to the $|q_1\rangle$ & $|q_2\rangle$ pair. The fidelity measurement of the entangled pairs $|q_0\rangle$ & $|q_3\rangle$, $|q_1\rangle$ & $|q_2\rangle$ using the equation (4.12) is equal to 0.9926 and 0.983.

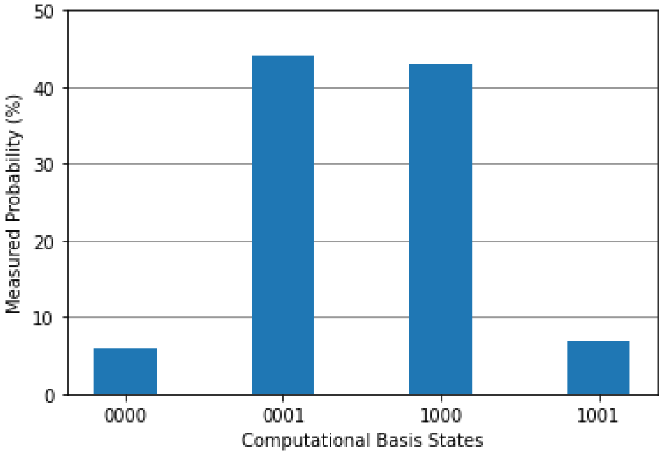


Figure 4.12: Probability measurement of the first and last entangled qubits ($|q_0\rangle$ & $|q_3\rangle$) in Quantum system

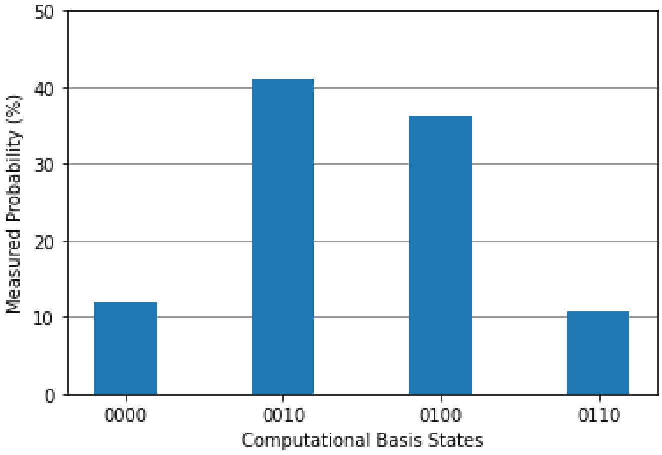


Figure 4.13: Probability measurement of the second and third entangled qubits ($|q_1\rangle$ & $|q_2\rangle$) in Quantum system

4.6.2 Result Analysis

In recent years, very few researchers have developed and executed quantum experiments on real quantum systems. From the literature, we found a paper Behera et al. (2019) where the authors implemented and experimented entanglement purification method in the IBM Quantum system using Greenberger–Horne–Zeilinger(GHZ) states. The rest of the papers (Yan et al., 2022; Zhang & Zheng, 2021; Huang et al., 2022) and many others are discussed the theoretical and simulator results. We compared the quantum results of the proposed entanglement purification method with the existing results Aleksandrowicz (2019), Behera et al. (2019). To perform entanglement purification, the authors performed entanglement swapping between the two entangled pairs. After applying swapping protocols, the fidelity of the resulting entangled pairs are 0.625 and

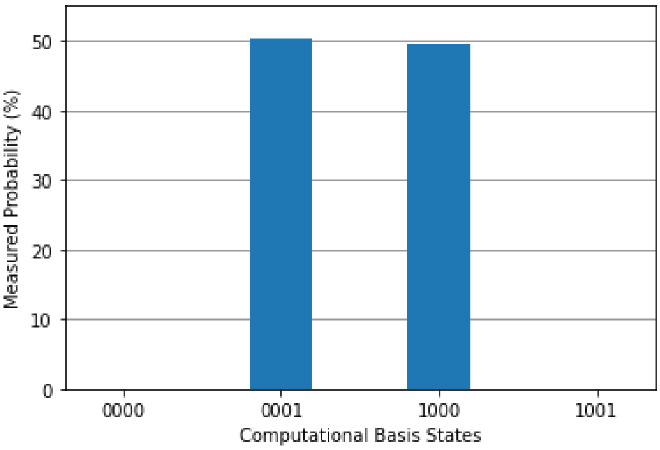


Figure 4.14: Probability measurement of the first and last entangled qubits ($|q_0\rangle$ & $|q_3\rangle$) in Quantum simulator

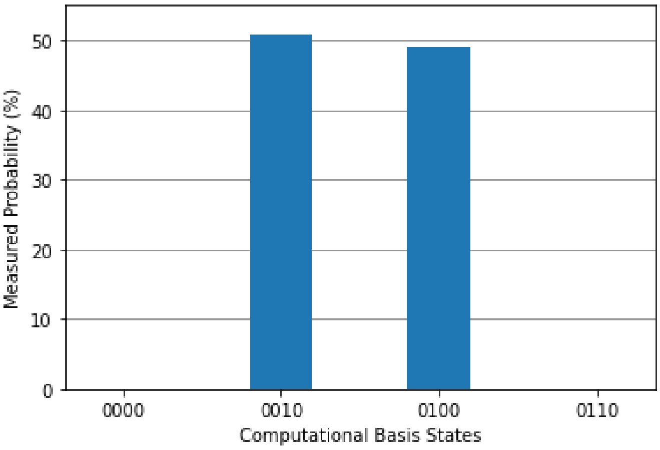


Figure 4.15: Probability measurement of the second and third entangled qubits ($|q_1\rangle$ & $|q_2\rangle$) in Quantum simulator

0.563, 0.8086 and 0.7840. The fidelity of the entangled pairs with the proposed entanglement swapping protocol are 0.8710 and 0.7720. In proposed method, entanglement has been swapped between $1^{st}, 4^{th}$ and $2^{nd}, 3^{rd}$ qubits. The proposed method also experimented on a Quantum simulator. The observed fidelity of the entangled pairs in the quantum simulator are 0.9926 and 0.983. We also compared the simulator results of the proposed method with existing works Yan et al. (2022); Zhang & Zheng (2021); Huang et al. (2022) and others. The Quantum system and Simulator result analysis of the proposed and existing methods are depicted in Figure 4.16 & 4.17.

From the analysis shown in Figures 4.16, 4.17, we can say that the proposed method gives efficient results compared to the existing ones. The proposed method is beneficial for efficient quantum communication and error correction. It mainly focuses on finding high-fidelity entangled pairs from weak ones. This method can also be helpful in various

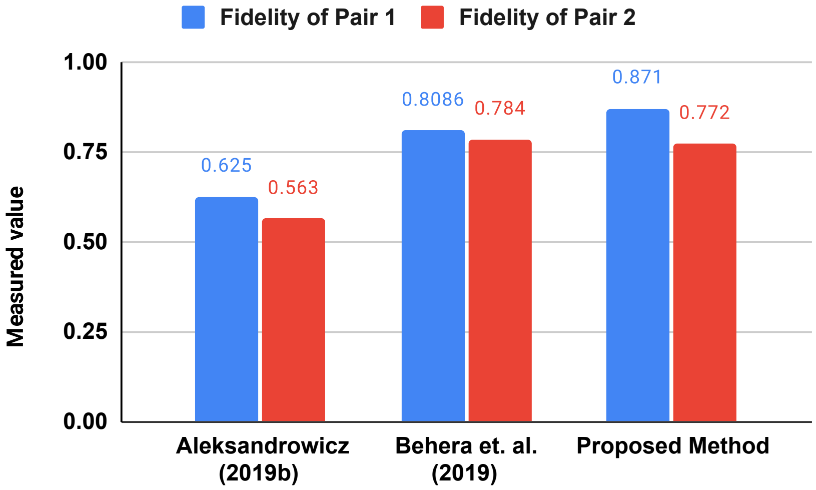


Figure 4.16: Fidelity Analysis of Existing and Proposed Methods with Quantum System Results.

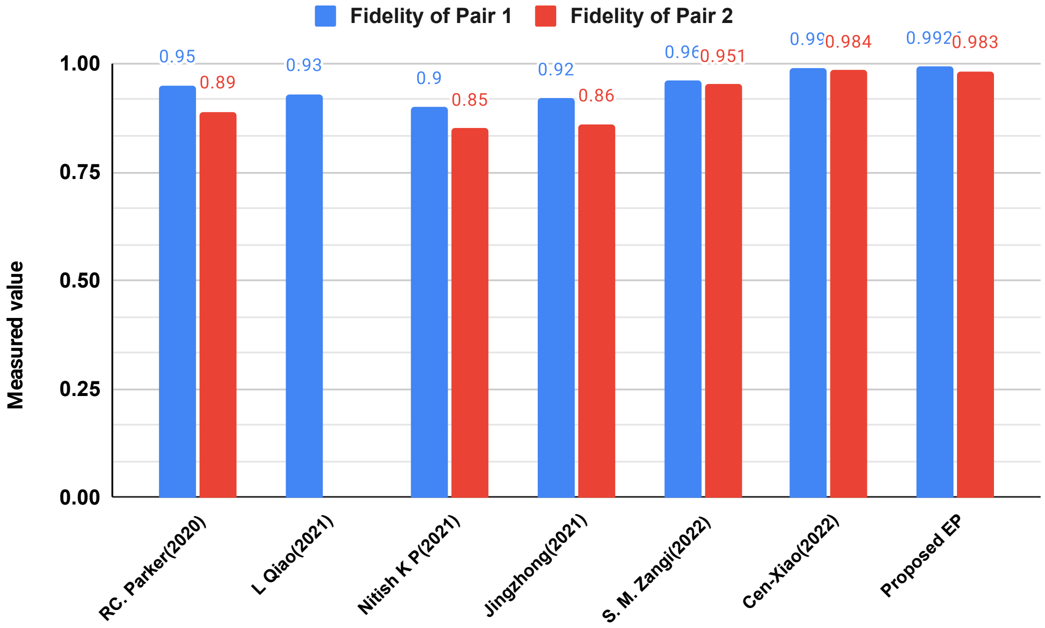


Figure 4.17: Fidelity Analysis of Existing and Proposed Methods with Simulator Results.

applications where data transmission is required for longer distances with less number of Hadamard and CNOT gates.

4.7 Summary

In this chapter, we proposed an efficient entanglement purification method using entanglement swapping. Entanglement purification distils the strong entangled pairs from weak ones. CNOT and Hadamard gates were used to develop the proposed Entanglement purification method. When the entanglement has been generated between two different pairs, it is observed that the fidelity of the entangled pair was less. After performing the swapping operation the fidelity of the entangled pair was increased to 0.8710 and 0.7720 in the quantum system and 0.9926 and 0.983 in the quantum simulator. From the quantum system and simulator results, it has been observed that the proposed architecture increases the fidelity of entangled pairs by reducing the system impurities when compared with the existing state-of-the-art methods. The proposed method is beneficial for efficient Quantum communication and Quantum error correction. This focuses on finding high-fidelity entangled pairs from weak ones. The maximally entangled pairs can be used in Quantum error correction models to develop efficient error detection and correction methods.

Chapter 5

Asymmetric Quantum Syndrome Error Correction

In the previous chapter, we discussed the entanglement purification method with entanglement generation and entanglement swapping operations. Entangled qubits play a significant role in Quantum Error Correction. In the following chapter, we explain in detail the Asymmetric Quantum Syndrome Error Correction with encoding, error correction and decoding operations. The role of entangled qubits in reducing the error rate and result analysis with the existing state-of-the-art methods were also detailed in this chapter.

5.1 Importance of Quantum Error Correction

Quantum Error Correction(QEC) is a principal resource for Quantum computation and communication. The current quantum systems are in the Noisy Intermediate Scale Quantum (NISQ) level (Singh Gill et al., 2020). The possibility of errors due to NISQ is bit and phase flips with the presence of noise and decoherence. Noise and decoherence arise when the qubits interact with the external environment while performing the operations (Hornberger, 2009). To address these issues and to reduce the error rate, Quantum Error Correction methods are required. Error detection and correction is an easy task in Quantum computation. As per the no-cloning theorem, it is not possible to copy the information. If we try to measure the error, its actual state will be disturbed (Wootters & Zurek, 1982). The existence of noise in the quantum system leads to errors like Bit flip errors (X), Phase flip errors (Z) and Bit & Phase flip errors (Y). The detailed discussion on Quantum errors with matrix representations are given in section 1.4. In order to detect and correct these errors and to reduce the error rate in Quantum Information Process (QIP), error correction methods need to be implemented (Hayashi, 2006).

5.2 Quantum Information Process (QIP) with Error Correction Method

The Quantum Information Process focuses on information process and computation by encoding information into quantum bits. QIP includes three major steps as depicted in Figure 5.1.

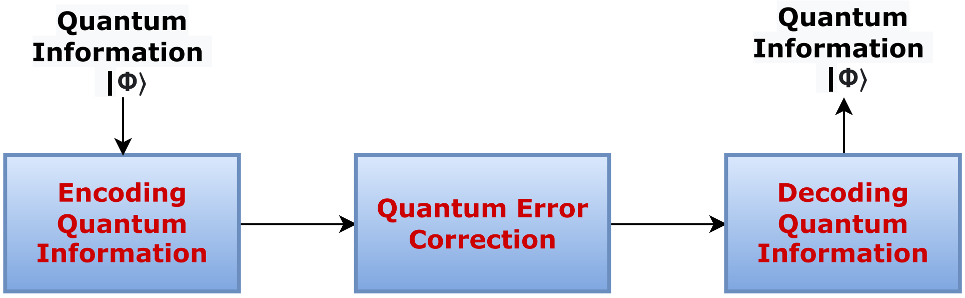


Figure 5.1: Quantum Information Process with error correction approach

As shown in Figure 5.1, logical qubits will be encoded into more number of physical qubits to process the information. If any error occurs while transmitting the information, that will be detected and corrected using the error correction process. After performing error correction, the information will be decoded into originally transmitted information by performing decoding operations. Based on this architecture, the QEC methods were implemented. Most of the quantum error correction methods are symmetric in nature. i.e. the symmetric methods are implemented by considering the probability of bit flip (X) and phase flip (Z) errors as the same (Wagner et al., 2018). From the literature (Ma et al., 2019; Chiani & Valentini, 2020b; Lv et al., 2021; Fan et al., 2021; Azad et al., 2021; Sundaresan et al., 2022), it has been observed that the possibility of phase shifts is more while transmitting the information. In order to overcome this problem, it is necessary to implement asymmetric quantum error correction methods. Thus, an efficient asymmetric quantum error correction method for detecting and correcting a single arbitrary error using syndrome measurement is proposed in this chapter.

Before discussing in detail about the proposed methodology, it is important to know about the phase operations, Quantum channel and Channel noise. Thus a detailed discussion of these topics is given in the following section.

5.3 Phase gate(S) and Unitary operations

5.3.1 S gate

S gate is used to modify the phase of a quantum state with 90-degree rotation along with the Z-axis to prevent phase shifts while encoding the information. It is a single input and single output gate (Zulehner et al., 2018).

The matrix representation of the S gate is $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{pmatrix}$

5.3.2 Unitary operation

It is also a single input and single output gate. A unitary gate performs the phase changes on a quantum state along with the X, Y, and Z-axis (Barabasi et al., 2019). For the experiment, we have considered phase angle as $\pi/4$ for better results as shown in the following equation.

$$U(\delta, \phi, \gamma) = RX(\delta - \pi/4)RY(\phi - \pi/4)RZ(\gamma - \pi/4) \tag{5.1}$$

Matrix representation of Unitary gate is $U(\delta, \phi, \gamma) = \begin{pmatrix} cos(\delta/2) & -e^{i\gamma}sin(\delta/2) \\ e^{i\phi}sin(\delta/2) & e^{i(\phi+\gamma)}cos(\delta/2) \end{pmatrix}$

5.4 Quantum Channel & Channel Noise

A Quantum channel is a transmission medium that is used to transmit quantum information from one place to another. When the quantum states are transmitted through the quantum channel, the noise will be generated due to the external interaction. In QIP two quantum channels will be used for data transmission which are called as the Depolarization quantum channel and the Amplitude damping channel. Based on the effect of transmitted quantum information on these quantum channels, the noise is divided into two types - Depolarization noise and Amplitude damping noise (Grassl et al., 2022).

5.4.1 Depolarization noise

When the information is transmitted through the Depolarization quantum channel, the noise will be generated and that leads to the depolarization noise. Depolarization noise does not completely destroy the quantum states but adds the bit and phase flip errors to the original information. It is also called as unitary noise. In the quantum channel, pure quantum states interact with the external environment which leads to mixed quantum states with different flip noises. There are three possible flip errors that arise due to the noise are represented in equation 1.19. A channel with depolarization noise can be described as follows.

$$\epsilon(\rho) = (1-p)\rho + \frac{p}{3}(\Gamma_x \rho \Gamma_x + \Gamma_y \rho \Gamma_y + \Gamma_z \rho \Gamma_z) \tag{5.2}$$

Where $\Gamma_x, \Gamma_y, \Gamma_z$ are the Pauli operators, p is the probability and ρ is the density operator of the input state in the quantum channel.

5.4.2 Amplitude Damping Noise

When the information is transmitted through an Amplitude damping quantum channel, the noise will be generated and that leads to the amplitude damping noise. Amplitude damping noise is also called as non-unitary noise where the entire quantum state will get disappeared. A Quantum channel with amplitude damping noise is represented as follows.

$$\epsilon(\rho) = \mathcal{A}_0 \rho \mathcal{A}_0^\dagger + \mathcal{A}_1 \rho \mathcal{A}_1^\dagger \tag{5.3}$$

Where $\mathcal{A}_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix}$ and $\mathcal{A}_1 = \begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix}$ are operational elements and ρ is density operator of the input state.

5.5 Proposed Methodology

Asymmetric quantum syndrome error correction architecture is capable of finding both bit and phase flip errors. It also prevents phase flips by performing phase operations on the encoding side. In the error correction method, three steps are to be performed, Those are Encoding, Error detection and correction using syndrome measurement, and Decoding. The overall architecture of the proposed Asymmetric Quantum Syndrome Error Correction (AQSEC) is represented in Figure 5.2.

Figure 5.2 shows the three major steps of the proposed AQSEC. Initially, an encoding operation is performed. In the encoding process, additional redundancy will be added in advance to handle the noise with extra qubits and quantum gate operations. After encoding the information $|\phi\rangle_E$, it will be transmitted through the quantum channel. If any error occurs while transmitting the information $|\phi\rangle_{Er}$, those will be measured using syndrome measurement with bounding function. After detecting and correcting the errors, the data will be decoded by performing decoding operations.

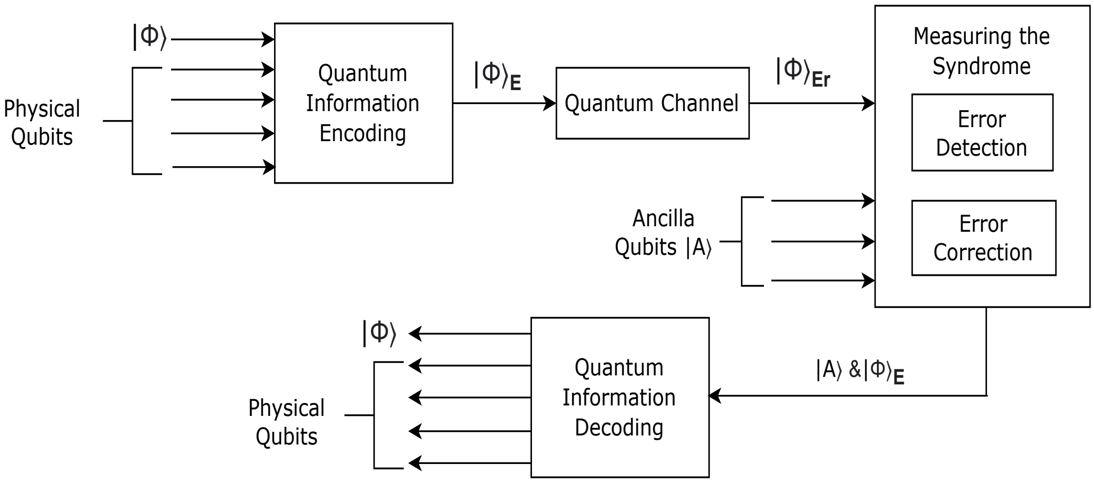


Figure 5.2: Asymmetric Quantum Error Correction with Encoding, Syndrome measurement, and Decoding procedure

5.5.1 Encoding the Quantum Information

To perform QEC, a single logical qubit is encoded into five physical qubits. In existing QEC methods, Hadamard (H) and phase shift (Z) gates are used for encoding the information. But in the proposed method, a single X gate is used to perform the HZH operations. We considered the logical quantum information that has to be transmitted as state $|1\rangle$. To encode the quantum information phase (S), Unitary (U) and Controlled-NOT operations are performed on the logical qubit. After performing S and Unitary operations on input data $|1\rangle$, the possibility of phase flip will be reduced. CNOT operations will be performed on logical data to encode it into five physical qubits. The mathematical representation of S, U, and CNOT operations on quantum state $|1\rangle$ are given below.

The S gate changes the phase of the input state with $\pi/2$ angle which is represented as follows.

$$S|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{\frac{i\pi}{2}}|1\rangle \tag{5.4}$$

Unitary operation on n quantum states with 2^n possible combinations can be derived as follows.

$$U^{2^n}|\tau\rangle \rightarrow e^{2i\pi\phi 2^n}|\tau\rangle \tag{5.5}$$

The above equation (5.5) is further simplified as follows for all possible operations.

$$
\begin{aligned}
U^{2^n}|\tau\rangle &\rightarrow \frac{1}{2^{\frac{n}{2}}}\sum_{l=0}^{2^n-1}|\gamma\rangle \otimes e^{2i\pi\phi l\tau}|\tau\rangle \\
&\rightarrow \frac{1}{2^{\frac{n}{2}}}[|0\rangle + e^{2i\pi\phi(2^n-1)}|1\rangle]
\end{aligned} \tag{5.6}
$$

Equation (5.6) represents all possible outputs with states $|0\rangle$ and $|1\rangle$. For input state $|0\rangle$, detecting phase changes is difficult because the phase change of $|0\rangle \rightarrow |0\rangle$. Therefore the phase modifications mainly affect the state $|1\rangle$. After applying unitary operations on input state $|1\rangle$ with $\pi/4$ angle, the above equation (5.6) will be modified as follows.

$$U|1\rangle \rightarrow e^{2\pi i\frac{\pi}{4}}|1\rangle \tag{5.7}$$

Equation (5.7) modifies the quantum state and prevents phase shifts in advance. If any phase shift occurs while transmitting the information, it can be detected by performing phase measurements using the following equation.

$$\text{Phase measurement} = \sqrt{1-p_r}|\gamma\rangle + e^{iP_h}\sqrt{p_r}|\tau\rangle \tag{5.8}$$

Equation (5.8) is used to calculate the phase of the quantum states $|\gamma\rangle, |\tau\rangle$ with probability p_r and phase P_h. For a quantum system with states $|0\rangle$ & $|1\rangle$, the above equation is modified as follows.

$$\text{Phase measurement} = \sqrt{1-p_r}|0\rangle + e^{iP_h}\sqrt{p_r}|1\rangle$$

The error rate is calculated using the formula $M(p_r) - E(p_r)$. It represents the difference between the maximum probability to the probability of the expected output state. After performing S and U operations on the quantum state, the CNOT gate will be applied to convert a single logical qubit into multiple physical qubits using the given equation.

$$\text{Encoded Information } \phi_E = \sum_i CNOT(|q_i\rangle, |q_{i+1}\rangle) \tag{5.9}$$

Here $|q_i\rangle, |q_{i+1}\rangle$ represents the Quantum states. The detailed algorithm for encoding quantum information using S, U and CNOT operations is represented in Algorithm 5.1.

Algorithm 5.1 Procedure for Encoding the Quantum Information

```
Input: Quantum Information $|\phi\rangle$
Output: Encoded Quantum Information $|\phi\rangle_E$
Initialize the number of qubits n as 5
Initialize Quantum register q and Classical register c with size 5
Apply NOT operation on initial qubit
Apply S and U operations along with X, Y, and Z axis
for $i = 0$ to $n - 2$ do
    Perform CNOT operation on q[i] & q[i+1]
end for
for $i = 0$ to $n - 1$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in the Classical register
Transmit the encoded information through the Depolarization Quantum Channel.
```

As written in Algorithm 5.1, a single logical qubit $|\phi\rangle$ is considered for transmitting from one end to another. To strengthen the logical information from noise and phase fluctuations, the S gate with angle $\pi/2$ has been applied to the initial qubit. It rotates the quantum state along the Z-axis with $\pi/2$ angle (as in equation 5.4). After that, the unitary operation with angle $\pi/4$ is applied on the same qubit to perform the rotation over the X, Y, and Z-axis (as in equation 5.1) to prevent the logical qubit from phase shifts. The combination of S and U gates leads to the U3 gate with the rotation along with X, Y, and Z gates with $3\pi/4, \pi/2$ and $\pi/2$ angles respectively. With these rotations, the phase of the quantum state will be maintained. To encode the logical qubit into five physical qubits, CNOT gate operations are performed. After encoding the quantum information, it will be transmitted through the depolarization quantum channel.

Algorithm 5.1 is developed and experimented on a quantum system. In the quantum system, the default input state will be considered as $|0\rangle$. It is difficult to measure the phase shifts on input state $|0\rangle$ because the phase shift on state $|0\rangle \rightarrow |0\rangle$ and for state $|1\rangle \rightarrow -|1\rangle$. Thus X gate is used to generate the input state as $|1\rangle$. After performing phase and unitary operations on qubit q[0], CNOT operations will be performed on q[0] & q[1], q[1] & q[2], q[2] & q[3], q[3] & q[4] to encode it into 5 qubits. After running the Algorithm 5.1 in a quantum system, the retrieved results for logical input $|1\rangle$ are shown in Figure 5.3. All possible quantum states of the proposed method with the achieved probabilities are represented with the density matrix in Figure 5.4.

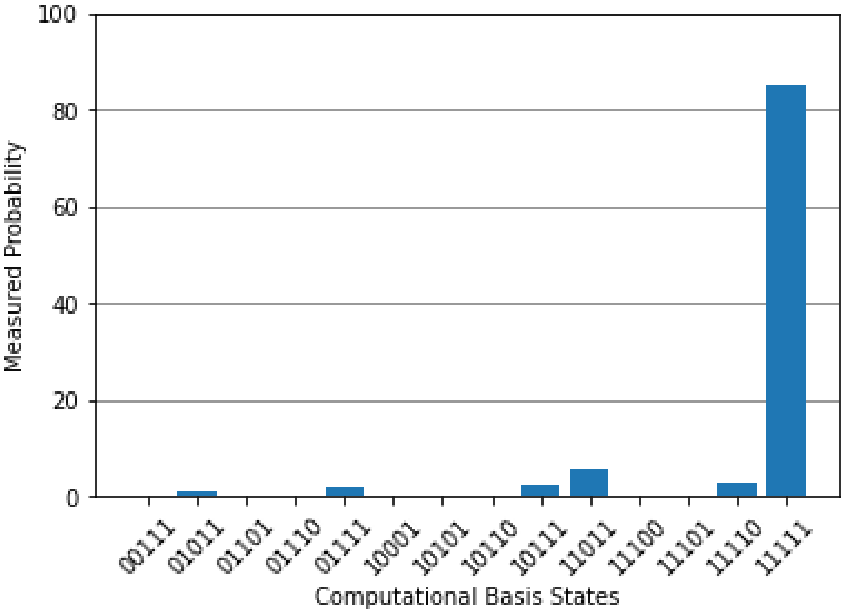


Figure 5.3: Quantum results for Encoding Quantum Information

The density matrix is used to represent all possible quantum states of the system with measured probabilities. Mathematically it is simplified by using the equation 1.18. For example, the possible outcomes of a single qubit system will be either $|0\rangle$ or $|1\rangle$. To represent all possible quantum states, the equation 1.18 is simplified with 2^1 states as follows

$$\rho = P_1|0\rangle\langle 0| + P_2|1\rangle\langle 1|$$

The vector simplification of the above equation results in the density matrix with all possible states with 2^1 x 2^1 matrix with probabilities P_1, P_2. For the n qubit system, the density matrix of all possible outcomes will be of size 2^n x 2^n. The calculated density matrix of the proposed encoding method with a 5-qubit system with a 32x32 matrix is graphically represented in Figure 5.4.

The error that is occurred due to the noise is measured by performing Positive Operator Value Measures (POVMs). POVM is used to measure the probability of a random outcome generated in quantum experiments. It is expressed as follows.

$$E_{rr} = (1 - P)|\phi_a\rangle\langle\phi_a| + P|\phi_b\rangle\langle\phi_b| \tag{5.10}$$

Here E_{rr} is the Error measurement and P represents the probability of error.

Bit and Phase error measurement probability for a two-qubit system with quantum

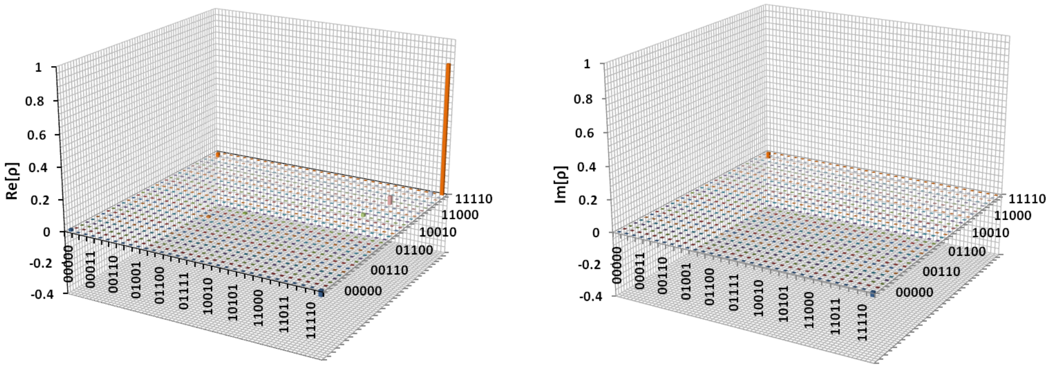
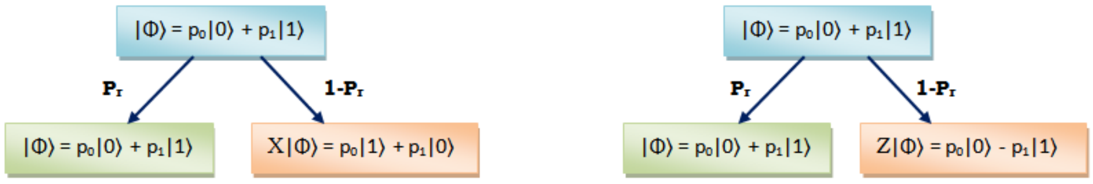


Figure 5.4: Density matrix of encoding method with all possible states with real and imaginary values Re[ρ], Im[ρ] respectively

states $|0\rangle, |1\rangle$ is graphically represented in the following figure.



a) b)

Figure 5.5: Bit and Phase error representations a) Represents the actual state $|\phi\rangle$ and bit flip of state $X|\phi\rangle$ with probabilities P_r and $1 - P_r$ b) Represents the actual state $|\phi\rangle$ and phase flip of state $Z|\phi\rangle$ with probabilities P_r and $1 - P_r$.

Figure 5.5 shows that, if the quantum information with state $|\phi\rangle = p_0|0\rangle + p_1|1\rangle$ has been transmitted through the quantum channel, then the qubit $X|\phi\rangle$ or phase $Z|\phi\rangle$ flips may occur with a probability of $1 - P_r$. According to this, the error measurement for the proposed encoding method is as in the following equation.

$$E_{rr} = (1 - P)|00000\rangle\langle 00000| + P|11111\rangle\langle 11111|$$

After running the encoding algorithm in a quantum computer, the resulting probability of state $|11111\rangle\langle 11111|$ is 0.852, i.e., P = 85.2%. From this we can calculate the error rate with equation 1-P = 0.148, i.e., 14.8%. The same result is expressed using the density matrix represented in Figure 5.4 with all noisy states. The proposed encoding method is also developed and executed on various quantum systems like Manila, Lima, Quito, Belem and so on to find an efficient quantum system to perform the experiments. From the results, it has been observed that the Manila system performs efficiently compared to other systems. A detailed analysis of various system results is presented in Appendix-A (refer the Appendix-A).

After encoding the information, the next step is to transmit the information through the quantum channel. For the experiment, we used IBM Quantum System. A depolarization quantum channel is used to transmit the information. As per the properties of the depolarization quantum channel, whenever the data is transmitted through this channel it may lead to the bit flip, phase flip, or bit and phase flip errors as discussed in 5.4.1. If any errors occur, those will be detected and corrected by performing error detection and correction operations.

5.5.2 Error Detection and Correction

Error detection and correction are two necessary and challenging steps in Quantum Information Process because the detection of phase flips is difficult. Before performing the error correction, it is essential to know the type of error due to which the encoded state has corrupted. This can be performed using syndrome measurements. Here the word syndrome represents the presence of an error and the error type, i.e., bit flip or phase flip or both and on which input state the error has occurred. Thus, the syndrome measurement is used to retrieve the error information like which Pauli error (X, Y or Z) has occurred and on which physical qubit. Based on this information error correction will be performed by applying the same Pauli operator on the corrupted qubit to revert the error effect.

Syndrome measurement and Error correction

To measure the syndrome five physical qubits will not be sufficient. Extra qubits are required to detect and correct the error. For that, 3-ancilla qubits $|A\rangle$ are used. Ancilla qubits are extra qubits that are used to perform intermediate operations and store partial results in quantum computation. Mainly ancilla qubits are used to convert complicated gate architectures into simple ones. In the proposed method, the combination of ancilla qubits is used to detect the error and also to find out exactly on which qubit it has occurred. Then the error correction will be performed to correct it. To perform these operations, we have considered hamming bound as a base and then it has been modified by considering the phase flips with the highest probability.

Bounding function calculation

CNOT operations are performed by applying hamming bound with parameters [n,k,d] for the detection of errors. Where n is the total number of physical qubits, k is the number of logical qubits and d is the distance between code words. Hamming bound represents the parameter limit for the arbitrary code. For example, if H_b is a set of symbols with b elements. The set of n length strings on H_b can be represented as H_b^n where it will have b^n distinct strings. The block code of b of length n is a subset of H_b^n. The hamming distance between code words can be represented as $H_b(n, d)$. It represents that the maximum size of block code with length n is b and the minimum hamming distance between code words is d. With these conditions, the hamming bound for code b^n with at least two distinct strings should satisfy the following equation.

$$H_b(n, d) \leqslant b^n / \sum_{w=0}^{t} \begin{pmatrix} n \\ w \end{pmatrix} (e-1)^w \tag{5.11}$$

Where t = $\frac{d-1}{2}$. The equation (5.11) is further simplified as follows.

$$H_b(n, d) \times \sum_{w=0}^{t} \begin{pmatrix} n \\ w \end{pmatrix} (e-1)^w \leqslant b^n$$

To satisfy the above equation the value of $H_b(n, d) = b^k$. Where k is the number of logical qubits. The modified equation after substituting $H_b(n, d) = b^k$ is as follows.

$$b^k \times \sum_{w=0}^{t} \begin{pmatrix} n \\ w \end{pmatrix} (e-1)^w \leqslant b^n$$

Here e represents all the possible non-trivial 1-qubit errors. The total number of possible 1-qubit errors are 4 (identity, bit, phase, bit and phase flips) as explained in equation (1.19). According to this, the above equation is simplified as follows.

$$b^k \times \sum_{w=0}^{t} \begin{pmatrix} n \\ w \end{pmatrix} 3^w \leqslant b^n$$

For 2-dimensional Hilbert space with n qubits, the above equation can be further simplified as follows.

$$2^k \times \sum_{w=0}^{t} \begin{pmatrix} n \\ w \end{pmatrix} 3^w \leqslant 2^n$$

To apply this bounding function, the minimum n value must be 5. After encoding the data, if any syndrome is observed while transmitting the information that can be measured and corrected with the help of the bounding function and CNOT operations. The step-by-step procedure for syndrome measurement with error correction is described in the following Algorithm 5.2.

Algorithm 5.2 Step by step procedure for Syndrome measurement

```
Input: Encoded Quantum Information transmitted through quantum channel $|\phi\rangle_{Er}$, Ancilla qubits $|A\rangle$
Output: Encoded information with the syndrome measurement $|A\rangle$ & $|\phi\rangle_E$
Initialize number of qubits n as 8
Initialize Quantum register q, Classical register c with size 5
Initialize Ancilla Register a with size 3
$q[0]$ & $q[(n/2)+1] \leftarrow$ Controlled NOT operation
$q[1]$ & $q[(n/2)+2] \leftarrow$ Controlled NOT operation
$q[2]$ & $q[(n/2)+1] \leftarrow$ Controlled NOT operation
$q[3]$ & $q[(n/2)+3] \leftarrow$ Controlled NOT operation
$q[2]$ & $q[(n/2)+2] \leftarrow$ Controlled NOT operation
$q[4]$ & $q[(n/2)+1] \leftarrow$ Controlled NOT operation
$q[4]$ & $q[(n/2)+3] \leftarrow$ Controlled NOT operation
for $i = (n/2)+1$ to $n-1$ do
    Store the information from Quantum register to Ancilla register
end for
Measure the information stored in Ancilla register
Initialize $A_r$ with the combination of Ancilla qubits
Measure the $A_r$
if $A_r! = 0$ then
    Add Pauli gate(s) on qubit
end if
for $i = 0$ to $n-1$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in the Classical register
```

After running the Algorithm 5.2 in Quantum computer with phase error at initial qubit q[0], the obtained results are depicted in Figure 5.6.

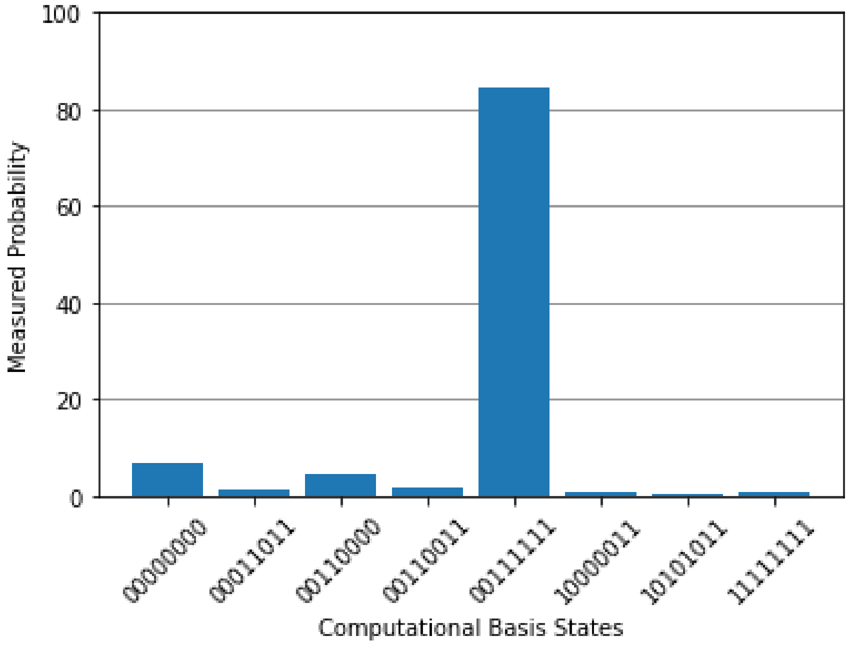


Figure 5.6: Quantum results for Syndrome measurement

As shown in Figure 5.6, the first 5 qubits (right to left) represent the encoded information and the remaining 3 qubits represent the ancilla qubits. To check the efficiency of the proposed algorithm, a phase error is added on the first qubit of the encoded information. After running the algorithm 5.6, the observed results contain the state $|00111111\rangle$ with maximum probability. The resulting state $|00111111\rangle$ represents that the error has occurred at first qubit q[0] with ancilla combination 001. CNOT operations are performed to detect and correct the error. The probability of the obtained result is 84.28%. Due to the noise quantum states $|00000000\rangle$, $|00011011\rangle$, $|00110000\rangle$ and so on are obtained. The measured error rate for the syndrome measurement algorithm using the equation (5.10) is 15.82%. After performing the error detection and correction, the next step is to decode the information into the original quantum information by performing decoding operations.

5.5.3 Decoding the Quantum Information

Decoding operation is very important for transmitting the information from one place to another. Even though the encoding and error correction operations show excellent results, if the decoder is unable to decode the originally transmitted information then the entire results will be affected. It may transmit the wrong information. In the proposed AQSEC, phase and unitary operations were performed along with CNOT gate operations to encode the information. Hence to decode the information, phase and unitary operations need to be performed. Therefore the encoding operations are performed in the backward direction to decode the originally transmitted information. After detecting and correcting the errors, the actual data will be decoded using the decoding operations as explained in algorithm 5.3.

Algorithm 5.3 Procedure for Decoding the Quantum Information

```
Input: Encoded information with the syndrome measurement $|A\rangle$ & $|\phi\rangle_E$
Output: The original information that has been shared initially $|\phi\rangle$
Initialize the number of qubits n as 5
Initialize Quantum register q, Classical register c with size 5
for $i = n - 1$ to 0 do
    Perform CNOT operation on q[i] & q[i-1]
end for
$q[0] \leftarrow$ Unitary operation
$q[0] \leftarrow S$
for $i = 0$ to $n - 1$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in the Classical register
```

After running the Algorithm 5.3 in a quantum system, the retrieved results in terms of probability measurement chart and density matrix are outlined in Figure 5.7 & 5.8.

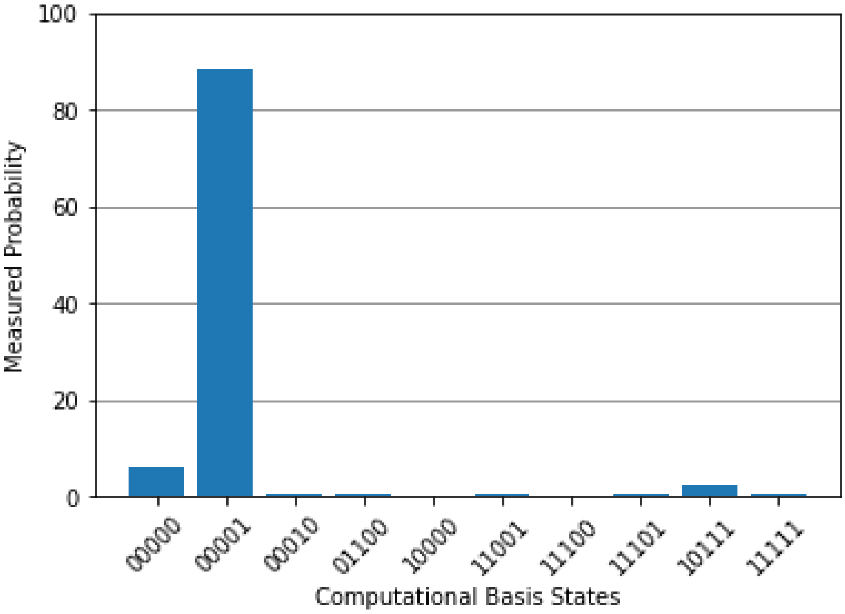


Figure 5.7: Quantum results for Decoding the quantum information

The initial input state considered for the proposed AQSEC is $|00001\rangle$ with logical qubit $|1\rangle$. After applying the encoding method, the state $|00001\rangle$ has been modified to $|11111\rangle$. By performing decoding operations, we obtained the same state as an output along with some noisy states as represented in Figure 5.7. From the results, it is observed that the proposed decoding algorithm achieved 88.3% probability with a 11.7% error rate. These are measured using the equation (5.10). The result of the final Quantum Error Correction algorithm by combining encoding, syndrome measurement, and decoding algorithms and the result analysis with existing works are discussed in the next section.

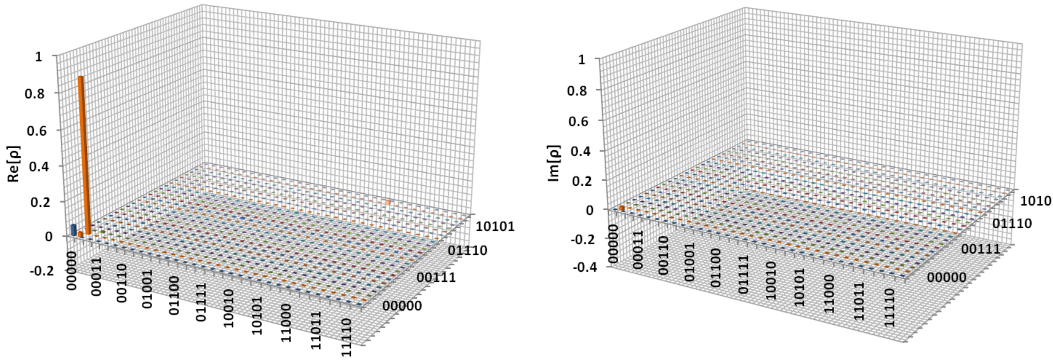


Figure 5.8: Density matrix of Decoding method with all possible states with real and imaginary values Re[ρ], Im[ρ] respectively

5.6 Experimental Setup

The classical and Quantum systems are used for performing the experiments. The configuration details of the Classical system are given below.

- Processor: Intel core I3
- RAM: 4GB
- Operating System: Windows 7 Ultimate

The proposed Asymmetric Quantum Syndrome Error Correction algorithm is developed and experimented on IBM Quantum System using the Qiskit tool. The configuration details of the IBM quantum system are as follows.

- System Name: ibmq_guadalupe
- Operating System: Darwin

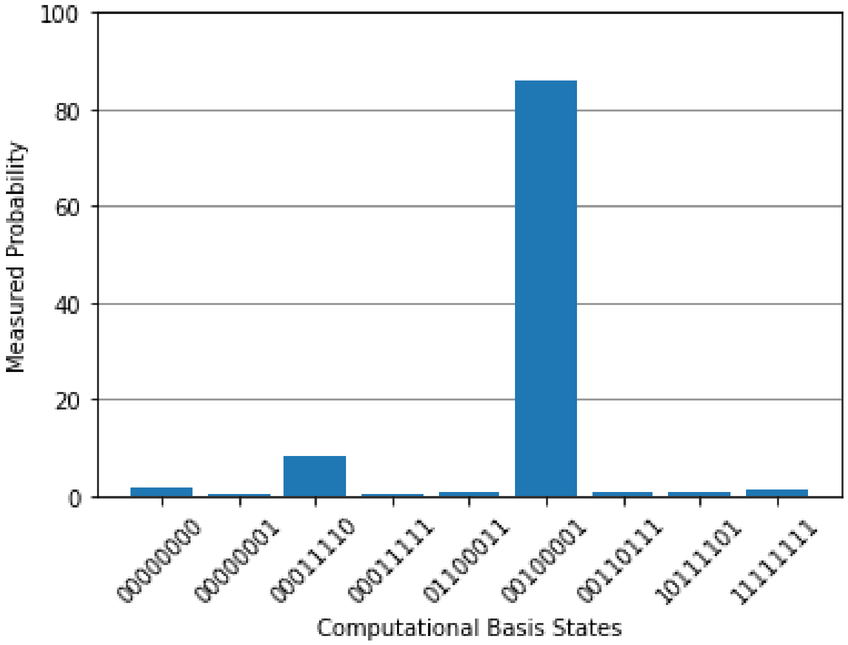


Figure 5.9: Quantum results for the proposed Asymmetric Quantum Syndrome Error Correction with Encoding, Error Detection & Correction and Decoding steps.

- Tool used: Qiskit tool
- Simulator: ibmq_qasm_simulator
- Processor: Falcon r5.11L

5.7 Discussion & Result Analysis

The proposed Asymmetric Quantum Syndrome Error Correction method is used to transmit the single logical qubit information using 5-physical qubits and 3-ancilla qubits. The overall algorithm of QEC contains the Encoding, Error detection & Correction using Syndrome measurement and Decoding operations. After running all these operations combinedly in the quantum system, the retrieved final output is shown in Figure 5.9.

The proposed AQSEC algorithm considers quantum state $|1\rangle$ as an input. To transmit this information, the encoding operation has been performed by adding extra physical qubits to strengthen the quantum information. After this operation, the output will be $|11111\rangle$. While transmitting the encoded information through the depolarization quantum channel, if any error occurs, it will be detected and corrected by performing syndrome measurement operations. The resulting state after performing this operation is $|00111110\rangle$, where it detects the error at qubit q[0]. After detecting the error, it will be corrected by performing CNOT and Pauli gate operations. The result after this step is $|00111111\rangle$. It represents the error detected and corrected at the first qubit. Finally, the data will be decoded by performing the decoding operations. The final output after this stage is $|00100001\rangle$ with 85.89% probability. In resulted state $|00100001\rangle$, the first five qubits represent the quantum information and the remaining three qubits represent ancilla qubits.

Fidelity Measurement

Fidelity is measured by using the mathematical formula $F = \langle\phi|\rho|\phi\rangle$ as in equation (4.12). Here $|\phi\rangle$ represents the expected output and ρ represents the density matrix of the resulting output. The value of ρ is calculated by using the equation $\sum_i p_i|\phi_i\rangle\langle\phi_i|$. Where $|\phi_i\rangle$ is resulted quantum state and p_i is the probability of the state $|\phi_i\rangle$. The resulted state $|\phi_i\rangle = |00100001\rangle$. The inner product of $|\phi_i\rangle = |\phi_i\rangle\langle\phi_i|$ will be performed on the $|\phi\rangle$ state vector. Here the outcome is of 8-qubits, so the vector of state $|\phi\rangle$ can be represented by 2^8x1 matrix. After simplifying equation F with the probability of the resulted state and the density matrix of size 2^8x2^8, the final outcome will be equal to 0.8589. Hence the fidelity of the proposed experiment is 0.8589. In the quantum system, we have calculated the fidelity of the proposed experiment using $qiskit.quantum\_info.state\_fidelity$ function.

Thus the retrieved results are efficient in terms of fidelity, number of ancilla qubits and circuit depth. Circuit depth is used to represent the number of quantum gates used in the longest path of a quantum operation. Quantum circuit depth represents the number of quantum gates in the circuit's longest path from the input to the output. In Qiskit, circuit depth is calculated by using $qiskit.circuit.QuantumCircuit.depth$ function. The circuit depth and the fidelity of the quantum operations are inversely proportional to each other. According to this, if the circuit depth is reduced, the fidelity will increase. The proposed QEC method produces an efficient result compared to the existing methods as represented in Figure 5.10.

From Figure 5.10, it is observed that the proposed QEC model improves the fidelity of the expected outcome with less number of ancilla qubits and reduced circuit depth.

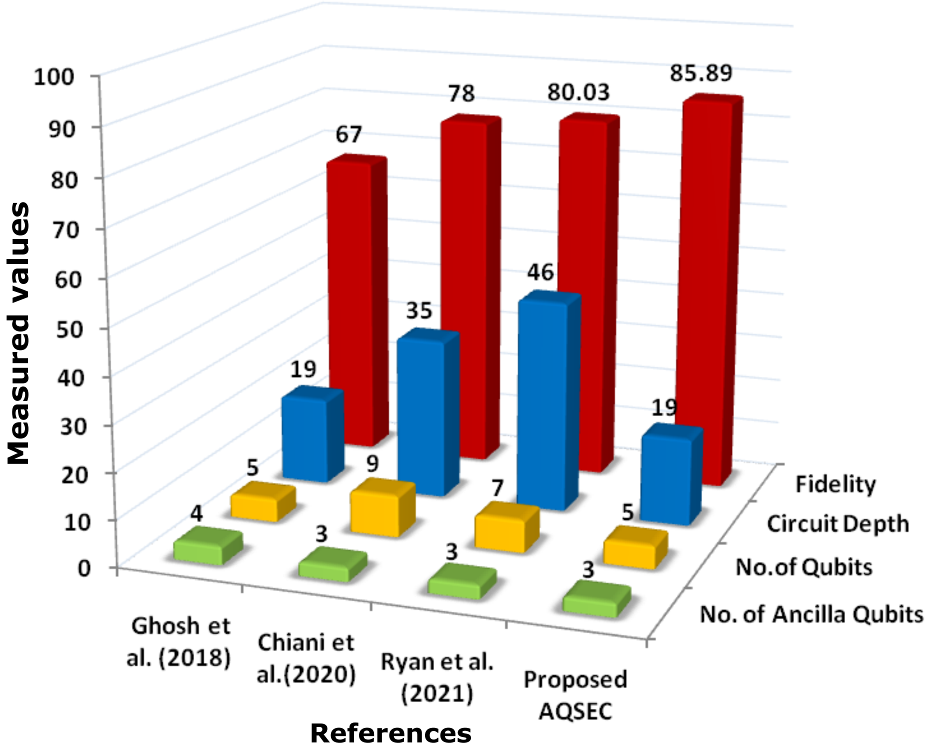


Figure 5.10: Result Analysis of proposed AQEC with existing methods

5.8 Asymmetric Quantum Syndrome Error Detection and Correction using Entangled qubits

Entanglement plays a crucial role in quantum error correction by providing a way to encode quantum information in a redundant manner. It allows for detecting and correcting errors that may occur during a computation. In a quantum system, the property of entanglement allows for the creation of correlations between qubits that are not possible in classical systems. These correlations can be used to encode quantum information in a more robust way against noise and errors. Thus, the entangled qubits are used in the proposed AQSEC to improve the performance and reduce the error rate. After adding the entangled qubits, the AQSEC architecture is modified as illustrated in Figure 5.11.

As depicted in Figure 5.11, Entanglement purification will be performed to purify the entanglement and generate the maximally entangled pair. These maximally entangled qubits are shared between the encoder and decoder to efficiently perform encoding and decoding operations on quantum information. Entangled qubits improve the efficiency of logical operations by reducing noise. To perform the error correction, the encoding operation will be performed on the initial qubit along with the entangled qubit.

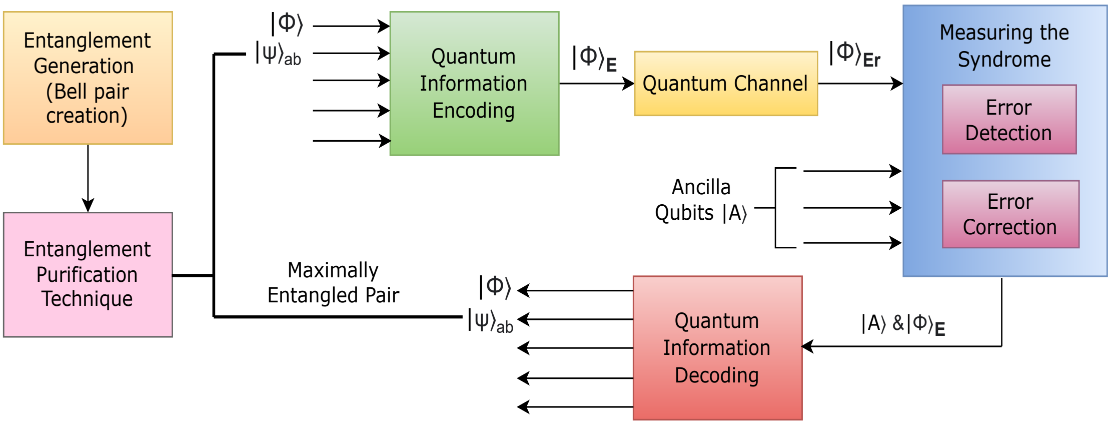


Figure 5.11: The process of Asymmetric Quantum Error Correction (AQEC) using Entanglement

The unitary and CNOT operations are performed on these qubits to generate physical qubits. The physical qubits are transmitted through the quantum channel after the encoding process. The quantum channel used here is depolarizing quantum channel. It leads to depolarization noise while transmitting the qubits. As a result, bit flip, phase flip or both errors may occur to the transmitted information. To detect and correct these errors, syndrome measurement will be performed using ancilla qubits. To perform the intermediate operations and store the partial results ancilla qubits are used along with the physical qubits. Finally, the decoding operation will be performed to get the initially transmitted information. The proposed AQSEC algorithm with entangled qubits is represented in Algorithm 5.4.

The result analysis of the proposed algorithm with the experimental setup is discussed in the following section.

5.8.1 Experimental Setup

The classical and Quantum systems are used for performing the experiments. The configuration details of the Classical system are given below.

- Processor: Intel core I3
- RAM: 4GB
- Operating System: Windows 7 Ultimate

The proposed algorithm is developed and experimented on IBM Quantum System using Qiskit tool. The configuration details of IBM quantum system are as follows.

Algorithm 5.4 Asymmetric Quantum Error Correction using Entangled Qubits

```
Input: Quantum Information $|\phi\rangle$
Output: Detection and correction of quantum errors in transmitted information
Initialize the number of qubits n as 8
Initialize Quantum register $Q_r$, Classical register $C_r$ with size 5
Initialize Ancilla register $A_r$ with size 3
Perform Hadamard and CNOT operations on qubits
Measure the entangled pairs of state $|\psi^{\pm}_{ab}\rangle$ or $|\phi^{\pm}_{ab}\rangle$
Perform bell state measurements
Perform NOT operation on second and fourth qubits
Perform CNOT operations on $Q_r[0,1],[0,2],[0,3]$
Perform H operation on $Q_r[0], Q_r[3]$
Perform CNOT operation on $Q_r[0,3]$
Measure the information stored in Classical register $C_r[0-3]$
Find the maximally entangled pair and share it between the encoding and decoding operations
Apply NOT operation on initial qubit
Apply S and U operations along with X,Y and Z axis on initial
Add entangled qubit $|\phi^{+}_{ab}\rangle$ to $Q_r[1]$
for $i = 0$ to $n-2$ do
    Perform CNOT operation on $Q_r[i]$ & $Q_r[i+1]$
end for
for $i = 0$ to $n-1$ do
    Store the information from the Quantum register to the Classical register
end for
Transmit the encoded information through the quantum channel.
Perform Controlled NOT operations on quantum states and store the result in quantum registers.
for $i = (n/2)+1$ to $n-1$ do
    Store the information from the Quantum register to the Ancilla register
end for
Measure the information stored in ancilla register
if $A_r! = 0$ then
    Add Pauli gates on qubit
end if
for $i = n-1$ to $0$ do
    Perform CNOT operation on $Q_r[i]$ & $Q_r[i-1]$
end for
$Q_r[0] \leftarrow$ Unitary operation
$Q_r[0] \leftarrow S$
$Q_r[1] \leftarrow |\phi^{+}_{ab}\rangle$
for $i = 0$ to $n-1$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in Classical register $C_r$
```

- System Name: ibmq_guadalupe
- Operating System: Darwin
- Tool used: Qiskit tool
- Simulator: ibmq_qasm_simulator
- Processor: Falcon r5.11L

5.8.2 Result Analysis

After running the Algorithm 5.4 in the quantum system and simulator, the observed results are depicted in Figure 5.12 & 5.13.

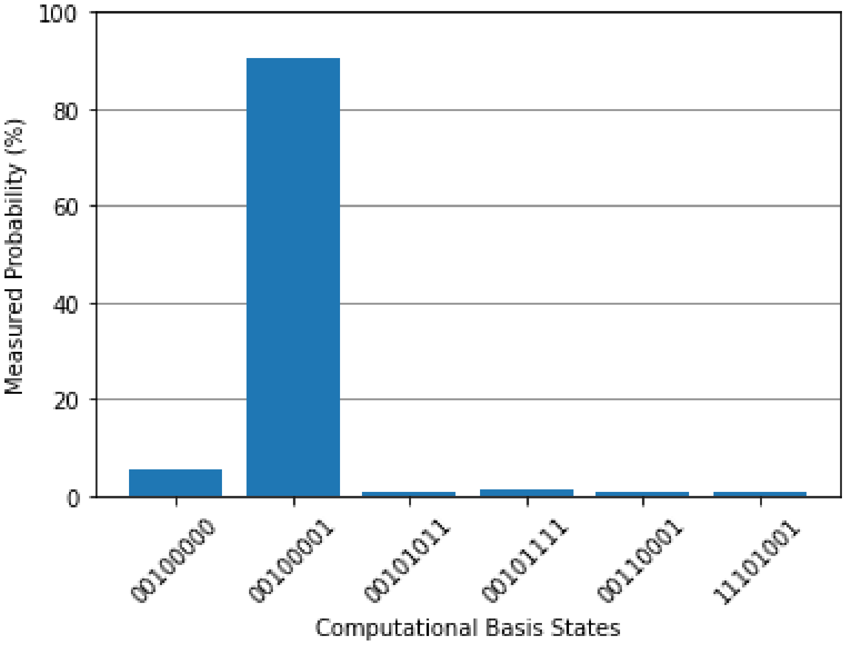


Figure 5.12: Quantum system result for AQSEC with Entangled qubits.

From Figure 5.12, it is observed that the measured probability of the proposed algorithm using equation (5.10) is 90.5%. The measured error rate is 9.5%, due to the noise that arises while performing the operations on qubits. The quantum state fidelity of the proposed algorithm is calculated using the equation (4.12), which is equal to 0.905. The experiment is also performed on a QASM simulator. From the simulator results as shown in Figure 5.13, it is observed that the fidelity of the resulting state is 0.9896. The retrieved results are efficient in terms of fidelity, number of ancilla qubits, and circuit

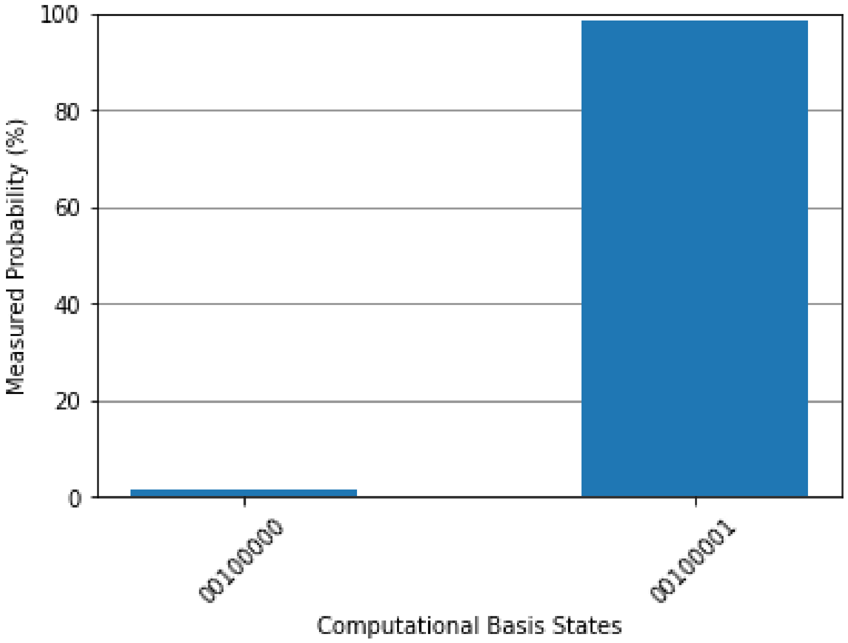


Figure 5.13: Quantum Simulator result for AQSEC with Entangled qubits.

depth. It also performed efficiently when compared to the proposed Asymmetric quantum syndrome error correction(AQSEC) algorithm with syndrome measurement. The result analysis with existing methods is represented in Figure 5.14.

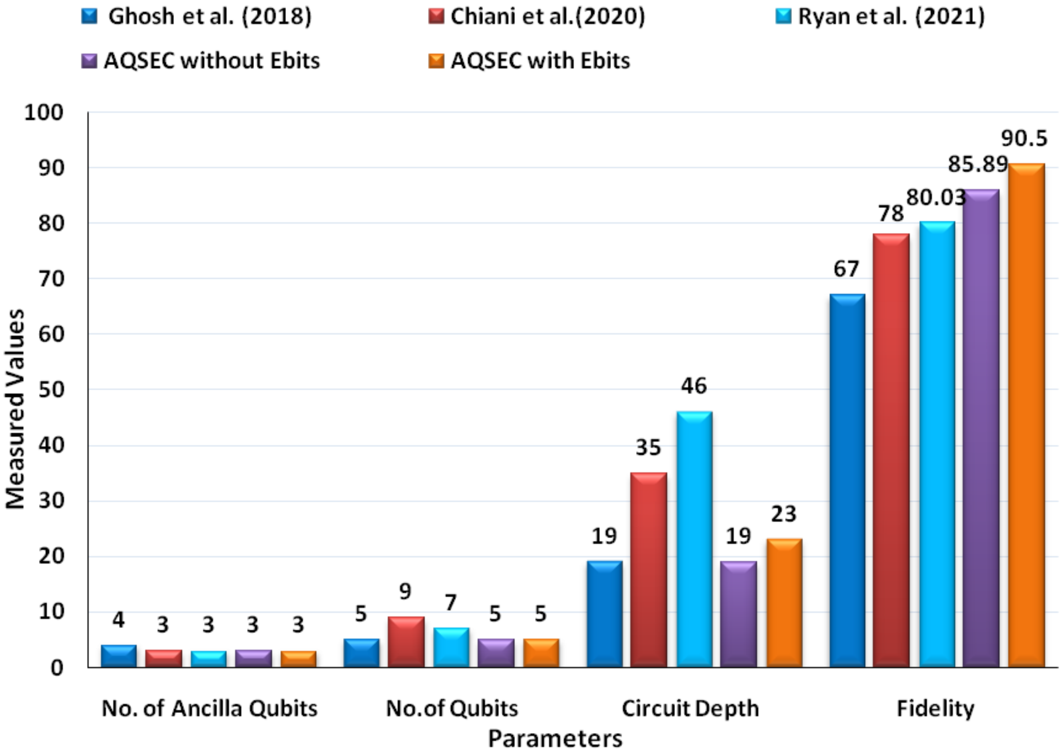


Figure 5.14: Result Analysis of proposed Asymmetric Quantum syndrome Error correction using Entangled Qubits with existing methods

Figure 5.14 shows that the proposed AQEC with entangled qubits improves the fidelity of the expected outcome with less number of ancilla qubits and reduced circuit depth. It also performed efficiently compared to the proposed AQSEC. The proposed method has also been experimented on a QASM simulator. From the experimental results shown in Figure 5.13, it has been observed that the achieved fidelity in the quantum simulator is 0.9896.

5.9 Summary

In this chapter, We have implemented a novel and efficient Asymmetric Quantum Error Correction (AQSEC) method with syndrome measurement with and without entangled qubits. The proposed AQSEC detects and corrects both bit and phase flip errors. The operations like encoding, decoding, and error correction are discussed clearly with algorithms. Syndrome measurement is performed using ancilla qubits to detect the type of error and on which qubit error has occurred. The required number of qubits in the proposed experiment is calculated using the bounding function. With the experimental results, it is observed that the proposed AQSEC outperforms when compared to the existing state-of-the-art methods. Further, to improve the efficiency of the proposed AQSEC, entangled qubits are used. The entangled qubits are shared at the encoder and decoder to perform the error correction. After running the Asymmetric Quantum Syndrome Error correction with entangled qubits in a quantum system, it has been observed that the final results are more efficient than the existing results. The experiments were also performed in the QASM simulator to test the methodology of the error correction mechanism. The results are analyzed in terms of fidelity, circuit depth and the number of qubits and ancilla qubits. It is also essential to optimize the architecture in terms of quantum cost. Quantum cost is used to measure the overall cost of the quantum architecture based on the number of quantum gates used in it. A detailed discussion of Quantum cost and Cost optimization methods is presented in the next chapter.

Chapter 6

Quantum Cost Optimization

In the previous chapter, we discussed the Importance of Asymmetric Quantum Syndrome Error Correction in the present era of Quantum Systems and the detailed process to develop an efficient AQSEC with entangled qubits. After developing an efficient QEC approach, it is important to check whether the model is cost-efficient or not. As a solution to this, it is necessary to develop quantum cost optimization methods. The following chapter discusses the quantum cost and cost optimization methods using reversible quantum gates. The main goal of this chapter is to propose efficient and optimized Entanglement purification and AQSEC methods.

6.1 Importance of Quantum Cost Optimization

Quantum cost optimization methods are essential as they allow the efficient and effective use of quantum resources in order to solve problems and perform specific tasks. In the field of quantum computing, cost optimization methods are used to minimize the number of quantum operations and quantum resources (such as qubits and quantum gates) that are required to solve a particular problem. Quantum computers are currently limited by the number of available qubits and the complexity of quantum circuits. This makes it important to minimize the use of quantum system resources by developing quantum cost optimization methods (Hogg & Portnov, 2000). Optimization methods are also crucial in the field of quantum communication as they are used to minimize the number of quantum states. Quantum operations that are required to transmit a message from one party to another. Because of it, quantum cost optimization methods are an important tool for maximizing the efficiency of quantum systems and are essential for enabling the practical use of quantum technologies in a wide range of applications. The operations performed in quantum systems are reversible (Mamun et al., 2014). Reversible computing performs the reversal of computational steps which allows the recovery of the original input data from the output data. This is achieved by designing algorithms and circuits that do not destroy the information or generate any entropy. Reversible computing has several potential benefits in the context of quantum computing. It helps to reduce the number of quantum resources required to implement a quantum algorithm, as reversible algorithms can be implemented using fewer qubits and gates than non-reversible algorithms. This is important to consider in the context of quantum cost optimization, as it allows to perform effective quantum operations. In addition to this, reversible computing will help to reduce the error rate in quantum algorithms. It eliminates the need for error correction and fault tolerance measures that are required in non-reversible algorithms (Banerjee & Pathak, 2009). This can be important for applications that require high accuracy and reliability such as Quantum cryptography, Quantum communication, Optical computing, Nanotechnology and scientific simulations. Reversible computing will enable the development of new quantum algorithms and applications that were previously thought to be impractical due to the high implementation cost. By finding ways to optimize the use of quantum resources through reversible computing, researchers can explore new areas of quantum computing and potentially discover new ways to solve various complex problems.

6.2 Quantum Cost and Unit cost Quantum gates

Classical computers perform irreversible operations in which the input information will be lost and unable to restore once the output is generated. Classical gates like AND, OR, EX-OR, NAND and NOR are irreversible gates with multi inputs and a single output (Caves, 1999). Reversible gates contain an equal number of inputs and outputs; each output is represented by a unique input combination. With this, it will be easy to restore the information in the case of data loss. Quantum gates like Fredkin, Feynman, Peres and Toffoli gates are reversible. The computational complexity of reversible logic gates is measured in terms of Quantum cost (Streltsov et al., 2012).

6.2.1 Quantum cost

The quantum cost of a reversible logic circuit is determined by the number of gates that are required to perform the desired operation. Quantum circuits need to be implemented by using low-cost quantum gates to develop cost-effective architectures. The Quantum cost of single input and single output (1x1) and two input and two output (2x2) gates is equal to 1 unit (Rahman et al., 2011). The cost increases with the increasing number of inputs and outputs. To optimize the quantum cost, higher-cost gates must be replaced with their equivalent lower-cost gates. The reversible gates like Hadamard (H), NOT, CNOT, Controlled-V, and Controlled-V^+ gates are unit cost gates. The Controlled-V, Controlled-V^+ gates are reversible gates and equivalent to quantum gates $Controlled-\sqrt{X}$ and $Controlled-\sqrt{X}^\dagger$ (Slimani et al., 2022). Every reversible gate is measured in terms of quantum cost. Reducing the quantum cost is a challenging task. Thus the research in this area has been increased to develop cost-effective architectures for various applications.

6.2.2 Unit cost Quantum Gates

A classical computer performs the operations with irreversible logic gates. In order to perform the operations in a Quantum computer, irreversible gates need to be converted into reversible gates. Reversible gates contain an equal number of inputs and outputs. The extra input and output lines will be added to the irreversible gates in order to convert them to reversible gates. The basic and fundamental reversible gates like NOT, CNOT, Controlled V and Controlled V^+ gates (Sasanian et al., 2012; Garipelly et al., 2013) are discussed in detail as follows.

NOT gate

NOT gate is a single input and single output gate. The operation of a reversible NOT gate is the same as the classical NOT gate. The output of this gate is the complement of its input. It means if the input is $|0\rangle$, the output is $|1\rangle$, and vice versa. NOT gate is represented with the symbol X. It is a unit-cost quantum gate.

CNOT gate

Controlled NOT or CNOT gate is a two-input (I_1, I_2) and two-output (O_1, O_2) gate. It is also called Feynman gate as represented in 1.3.2. The Quantum cost of this gate is equal to 1 unit.

Controlled V and V^+ gates

Controlled V and V^+ gates are two input (I_1, I_2) and two output (O_1, O_2) gates. The Quantum cost of these gates is equal to 1. The block diagram of Controlled V and V^+ gates are illustrated in Figure 6.1.

As shown in Figure 6.1, The first output of Controlled V and V^+ gates are equal to its first input, i.e. O_1 = I_1. The second output of the controlled V gate depends on its

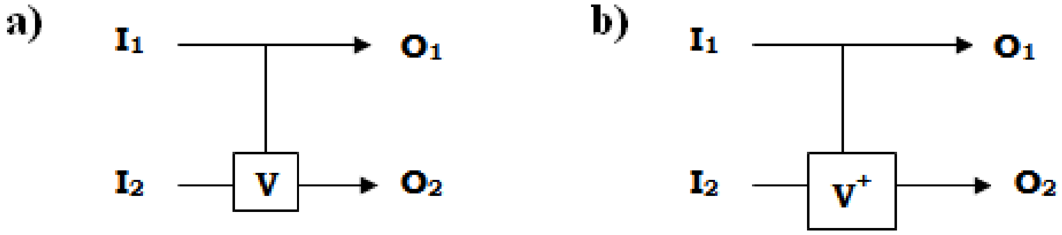


Figure 6.1: a) Controlled V gate b) Controlled V^+ gate

first input, i.e. if I_1 = 0 then O_2 = I_2, otherwise O_2 = $V(I_2)$. Similarly for controlled V^+ gate O_2 = $V^+(I_2)$ for I_1 = 1.

V and V^+ are calculated by using the equations $\frac{(i+1)}{2} * \left(\begin{smallmatrix} 1 & -i \\ -i & 1 \end{smallmatrix}\right)$ and $\frac{(-i+1)}{2} * \left(\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right)$. From these equations, we can say that $V^+ = V^{-1}$. The quantum cost of these gates is equal to 1 unit. The quantum cost of other single input and single output gates like Hadamard gate (H), Phase gate, and unitary gate is equal to 1 unit.

$\sqrt{x}$ gate and $\sqrt{x}^\dagger$ gate

In quantum, V gate is represented with $\sqrt{x}$ gate and V^+ gate is represented with $\sqrt{x}^\dagger$ gate. $\sqrt{x}$, $\sqrt{x}^\dagger$ gates are single qubit gates with unit cost. The matrix representation of these gates is as follows:

$$\sqrt{x} = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}, \sqrt{x}^\dagger = \frac{1}{2} \begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} \tag{6.1}$$

$\sqrt{x}$, $\sqrt{x}^\dagger$ gates are useful in optimizing the reversible circuits. The properties of these gates are represented in the form of lemmas as follows:

Lemma 6.2.1. *Consider a quantum $\sqrt{x}$, $\sqrt{x}^\dagger$ gates. The multiplication between these two gates produces the Identity gate.*

To prove this the operations are to be performed using matrix representation of $\sqrt{x}$, $\sqrt{x}^\dagger$ gates as follows.

$$\sqrt{x} * \sqrt{x}^\dagger = \frac{1}{2} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} * \frac{1}{2} \begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix}$$

$$
\begin{aligned}
\sqrt{x} * \sqrt{x}^{\dagger} &= \frac{1}{4}\begin{bmatrix} 2-2i^2 & 2+2i^2 \\ 2+2i^2 & 2-2i^2 \end{bmatrix} \\
&= \frac{1}{4}\begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
&= \text{Identity gate}
\end{aligned}
$$

Lemma 6.2.2. *Consider a quantum* $\sqrt{x}^{\dagger}$ *gate. The multiplication between two* $\sqrt{x}^{\dagger}$ *gates is equal to the Quantum NOT gate.*

To prove this the operations need to be performed using a matrix representation of $\sqrt{x}^{\dagger}$ gate as follows.

$$
\begin{aligned}
\sqrt{x}^{\dagger} * \sqrt{x}^{\dagger} &= \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} * \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} \\
&= \frac{1}{4}\begin{bmatrix} 2+2i^2 & 2-2i^2 \\ 2-2i^2 & 2+2i^2 \end{bmatrix} \\
&= \frac{1}{4}\begin{bmatrix} 0 & 4 \\ 4 & 0 \end{bmatrix} \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
&= \text{NOT gate}
\end{aligned}
$$

The quantum cost optimization algorithms for various reversible logic gates using unit cost quantum gates are discussed in the following section.

6.3 Proposed methodology for Quantum cost optimization

The optimization algorithms are used to develop cost and energy-efficient circuits. Quantum gates like the Double Feynman gate, Fredkin gate, Peres gate, and Toffoli gates are used to develop sequential circuits. All these are three input and three output gates with a quantum cost of 5 units. The cost-effective sequential circuits can be designed by optimizing above mentioned gates using low-cost quantum gates. The proposed methodology for the quantum cost optimization algorithm is depicted in Figure 6.2.

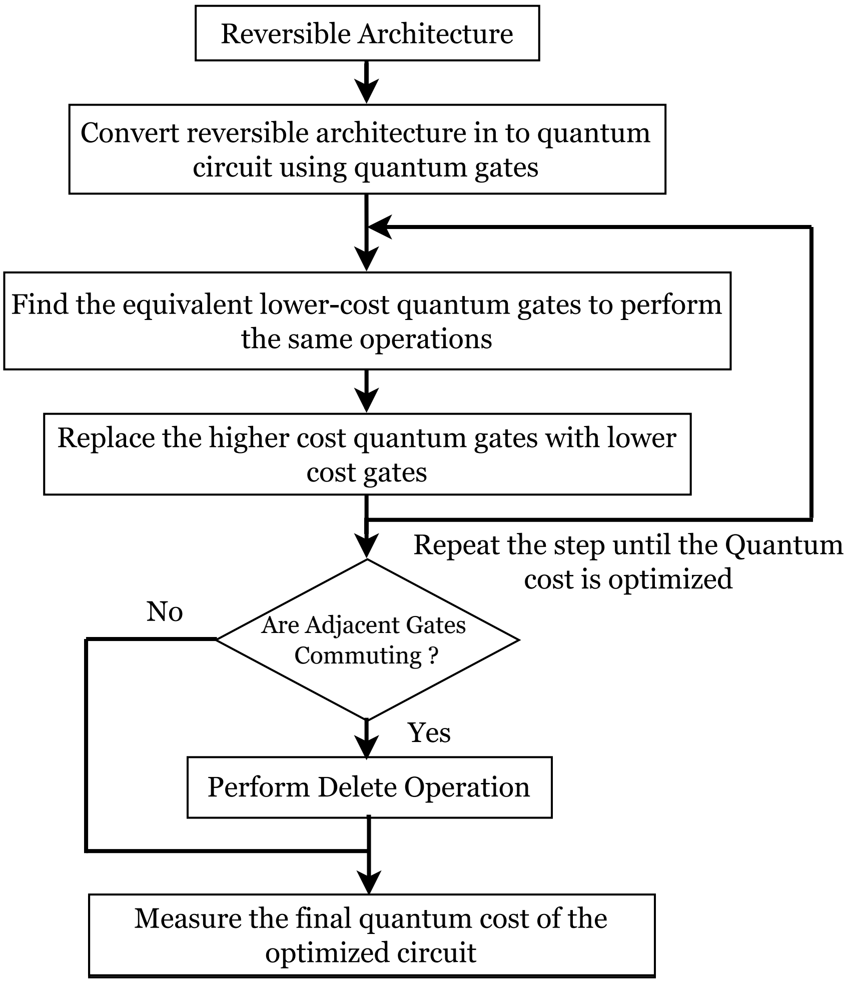

Reversible Architecture
Convert reversible architecture in to quantum circuit using quantum gates
Find the equivalent lower-cost quantum gates to perform the same operations
Replace the higher cost quantum gates with lower cost gates
Repeat the step until the Quantum cost is optimized
No
Are Adjacent Gates Commuting ?
Yes
Perform Delete Operation
Measure the final quantum cost of the optimized circuit

Figure 6.2: Procedure for Quantum Cost Optimization

As shown in Figure 6.2, to optimize the quantum cost, initially reversible architectures will be converted into quantum circuits using fundamental quantum gates. If the quantum cost of the circuit is high, then that will be reduced by replacing the higher-cost quantum gates with equivalent lower-cost gates. This step will be repeated until the higher-cost quantum gates are replaced with possible lower-cost gates. After that, it is necessary to observe the adjacent gates. If they are commuting, then the delete operation will be performed. Adjacent gate commuting refers to the property of certain quantum gates to commute with one another when they are applied to adjacent qubits.

Commuting gates are gates that can be applied in any order without changing the overall result. In other words, if two gates are commuting, then the order in which they are applied does not matter. In such cases, the deletion operation can be performed to delete any one of the commuting gates to minimize the number of gates that are required to perform operations. The optimized cost of the circuit will be measured after performing these operations. This procedure can be used to optimize the quantum or reversible architectures in order to reduce the hardware requirements. We have applied the proposed optimization algorithm on the entanglement purification method (discussed in Chapter 4), AQSEC (discussed in Chapter 5) and higher cost quantum gates like Toffoli and Peres gates to minimize the cost. The proposed algorithms for the same are discussed in the following sections.

6.3.1 Optimization algorithm for Toffoli gate

Toffoli gate is a three input (I_0, I_1, I_2) and three output (O_0, O_1, O_2) gate. Each output is calculated using unique input combinations which are expressed with the equations $O_0 = I_0, O_1 = I_1, O_2 = I_0 I_1 \oplus I_2$. The block diagram of the Toffoli gate is illustrated in Figure 6.3.

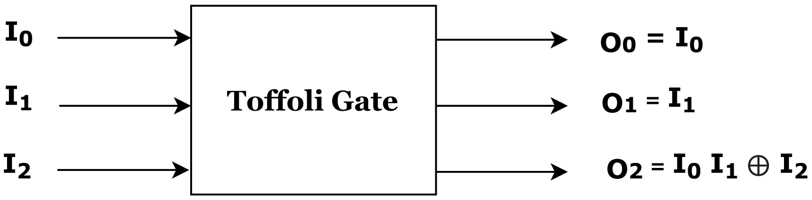


Figure 6.3: Block diagram of Toffoli gate

The quantum cost of the Toffoli gate is five units. This gate plays an important role in implementing various gates like TR, Fredkin, Peres, R gates and sequential circuits. The optimized Toffoli gate will be helpful in designing cost-optimized quantum circuits. The quantum circuit diagram for the Toffoli gate is shown in Figure 6.4.

The proposed optimization algorithm for the Toffoli gate with unit cost gates is given below.

The Algorithm 6.1 performs the Toffoli gate operations with the two $Controlled - \sqrt{X}$ gates(csx) and one CNOT and sxdg gate. CNOT gate is a two-input and two output gate and csx, sxdg gates are one input and one output gate with unit quantum cost. The

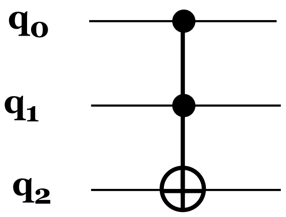


Figure 6.4: Quantum Circuit diagram of Toffoli gate. Here q_0, q_1, q_2 represents the quantum states

Algorithm 6.1 Optimization algorithm for Toffoli gate

```
Input: Three Inputs
Output: Three Outputs
Initialize the number of qubits n as 3
Initialize the size of Quantum register q and Classical register c as 3
Perform csx operation on q[1],q[2]
Perform csx operation on q[0],q[2]
Perform sxdg operation on q[2]
Perform cx operation on q[0],q[1]
Store the output in the Classical register
Measure the information stored in the Classical register
```

overall quantum cost of the optimized Toffoli gate is reduced to 4 units compared to the existing one which is of 5 units. After running the algorithm for input combination $|010\rangle$ in a quantum system, the retrieved results are exemplified in Figure 6.5.

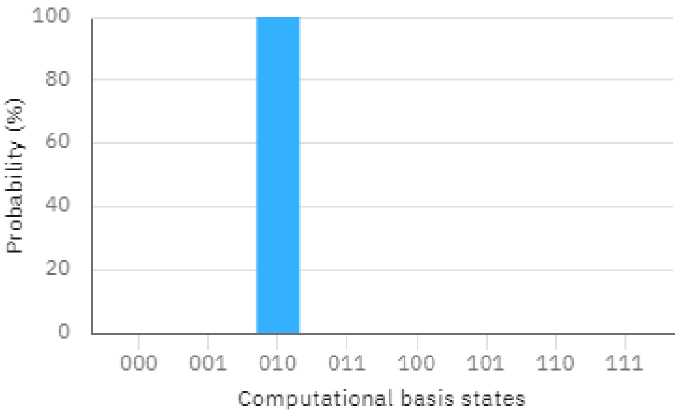


Figure 6.5: State vector diagram of Optimized Toffoli gate algorithm in Quantum system for input combination $|010\rangle$.

From Figure 6.5, it has been observed that the optimized gate performs the Toffoli gate operations efficiently using the low-cost quantum gates. It also optimizes the quantum depth. Quantum depth is used to measure the total number of gates in the longest path from input to output.

6.3.2 Optimization algorithm for Peres gate

Peres gate is a three input (I_0, I_1, I_2) and three output (O_0, O_1, O_2) gate. Each output is represented using the unique input combinations as expressed with the equations $O_0 = I_0, O_1 = I_0 \oplus I_1, O_2 = I_0 I_1 \oplus I_2$. The block diagram of the Peres gate is illustrated in Figure 6.6.

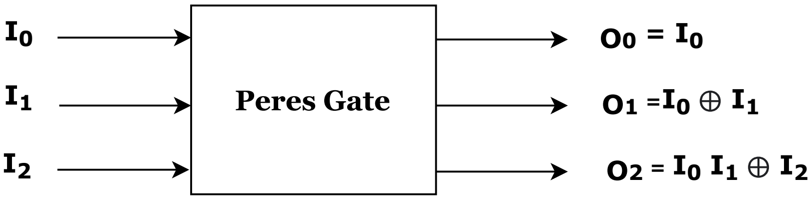


Figure 6.6: Block diagram of Peres gate

Peres gate is developed by using Toffoli and CNOT gates. The quantum cost of Peres gate is six units. Peres gate plays an important role in implementing quantum memory architectures. The optimized Peres is useful for designing cost-optimized circuits. The quantum circuit diagram for Peres gate is depicted in Figure 6.7.

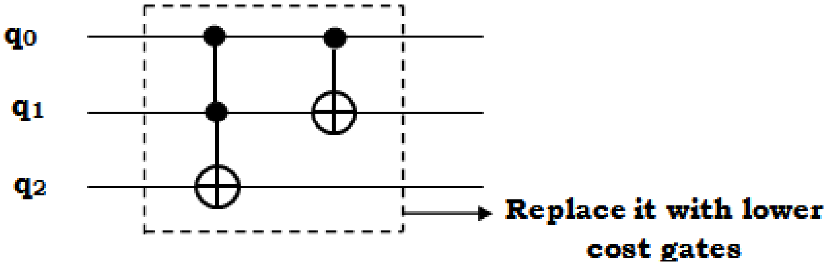


Figure 6.7: Quantum Circuit diagram of Peres gate

The optimized Toffoli gate is used to optimize the cost of the Peres gate. The proposed optimization algorithm for Peres gate using unit cost gates is given below.

The Algorithm 6.2 performs the Peres gate operations with the two $controlled-\sqrt{X}$ (csx) and controlled-NOT gates(cx) and one $\sqrt{X}^\dagger$ gate(sxdg). csx, sxdg gates are single input and single output gates and cx is a two input and two output gate with unit quantum cost. Thus the overall quantum cost of the optimized Peres gate is 5 units which is less compared to the existing one with 6 units. After running the Algorithm 6.2 for input combination $|001\rangle$ in a quantum system, the retrieved results are depicted in Figure 6.8.

Algorithm 6.2 Optimization algorithm for Peres

```
    Input: Three Inputs
    Output: Three Outputs
1: Initialize the number of qubits n as 3
2: Initialize the size of Quantum register q and Classical register c as 3
3: Perform csx operation on q[1],q[2]
4: Perform csx operation on q[0],q[2]
5: Perform cx operation on q[0],q[1]
6: Perform sxdg operation on q[2]
7: Perform cx operation on q[0],q[1]
8: Store the output in Classical registers
9: Measure the information stored in the Classical register
```

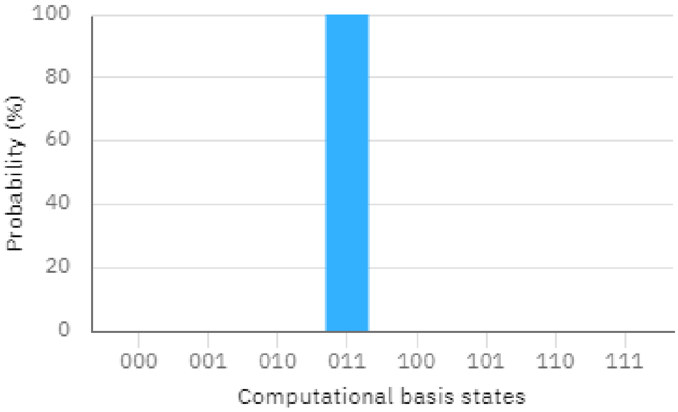


Figure 6.8: State vector diagram of Optimized Peres gate algorithm in Quantum system for input combination $|001\rangle$.

From Figure 6.8, it has been observed that the optimized gate performs the Peres gate operations with unit cost quantum gates. It also optimizes the quantum depth. With the help of unit cost gates, it is also possible to optimize the quantum cost of reversible gates like Fredkin gate, TR gate, etc to reduce the overall cost of the circuits.

6.3.3 Optimization algorithm for Entanglement purification method

Entanglement purification is an important tool for maintaining the integrity of quantum states and is essential for the reliable storage and transmission of quantum information. It is especially used to create highly entangled quantum states to perform quantum error correction. Highly entangled quantum states are essential for getting efficient results while performing the operations. For that, we proposed an efficient entanglement purification (EP) method in Chapter 4. The algorithm for the proposed EP is represented in Algorithm 4.1.

As mentioned in Algorithm 4.1, CNOT and Hadamard Operations were performed to generate the entanglement and purify it. After applying the proposed optimization method on Algorithm 4.1, it is observed that the CNOT gates are commuting. The commuted CNOT gates are removed by performing a deletion operation. It leads to the optimization of quantum cost. The proposed optimization algorithm EP method is as follows.

Algorithm 6.3 Optimization algorithm for Entanglement purification

```
Input: Two entangled pairs
Output: Maximally entangled pair
Initialize Quantum Register q[] with size 4
Initialize Classical Register c[] with size 4
Initialize the Number of qubits n as 4
$q[1] \leftarrow X$
$q[3] \leftarrow X$
Perform H operation on q[0]
Perform CNOT operation on q[0], q[1]
Perform H operation on q[2]
Perform CNOT operation on q[2], q[3]
Perform H operation on q[0]
$q[2] \leftarrow H$
$q[0] \leftarrow H$
Perform CNOT operation on q[0], q[3]
Perform CNOT operation on q[3], q[0]
Perform CNOT operation on q[0], q[3]
$q[2] \leftarrow H$
Perform CNOT operation on q[1], q[2]
Perform CNOT operation on q[2], q[1]
Perform CNOT operation on q[1], q[2]
for i=0 to n-1 do
    $c[i] \leftarrow q[i]$
end for
for i=0 to n-1 do
    Measure c[i]
end for
```

To optimize the entanglement purification algorithm, commuting CNOT gate operations are removed. After running the Algorithm 6.3 in a quantum system, it is observed that the proposed algorithm performs the entanglement purification with less number of quantum gates with better efficiency. The results of the quantum system are illustrated in Figures 6.9 & 6.10.

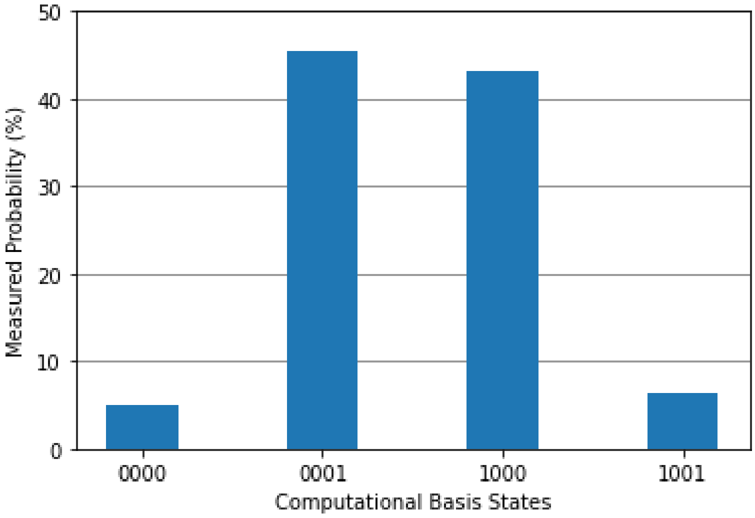


Figure 6.9: Quantum system Results of Entangled pair [q0,q3]

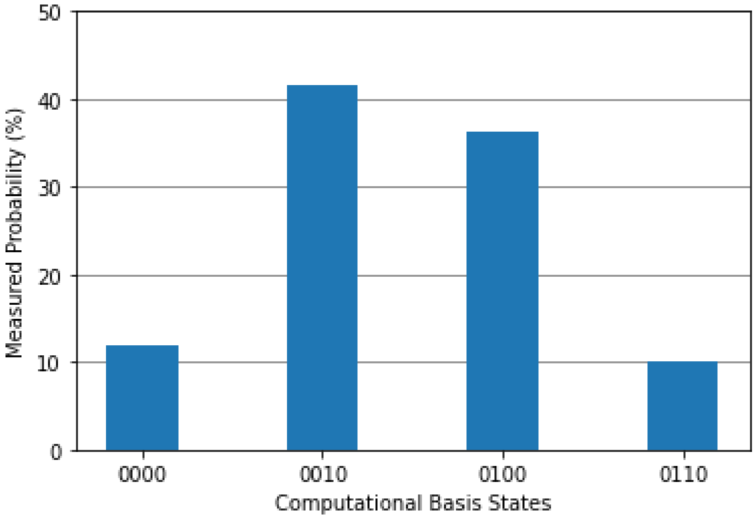


Figure 6.10: Quantum system Results of Entangled pair [q1,q2]

From Figures 6.9 & 6.10, it is observed that the fidelity of the pair [q0,q3] is 0.887 and pair [q1,q2] is 0.7792.

6.3.4 Optimization algorithm for Entanglement based Asymmetric Quantum Error Correction

Quantum error correction plays a crucial role in Quantum Information Process. Moreover, the error rate is high in quantum computing due to the delicacy of quantum particles. When the operations are performed on quantum particles, it results in noise and decoherence due to external interactions. Because of these, the error rate increases which in turn results in information loss. Error correction strategies are performed in order to overcome this issue. with the experimental results of chapter 5, it has been observed that the asymmetric quantum error correction with entangled qubits performs efficiently in detecting and correcting the errors while transmitting the information. We considered the entanglement-based quantum error correction method and applied the optimization techniques as per figure 6.2 in order to optimize it. After applying all the steps, it has been observed that the entanglement-based quantum error correction can be optimized further as depicted in Figure 6.11.

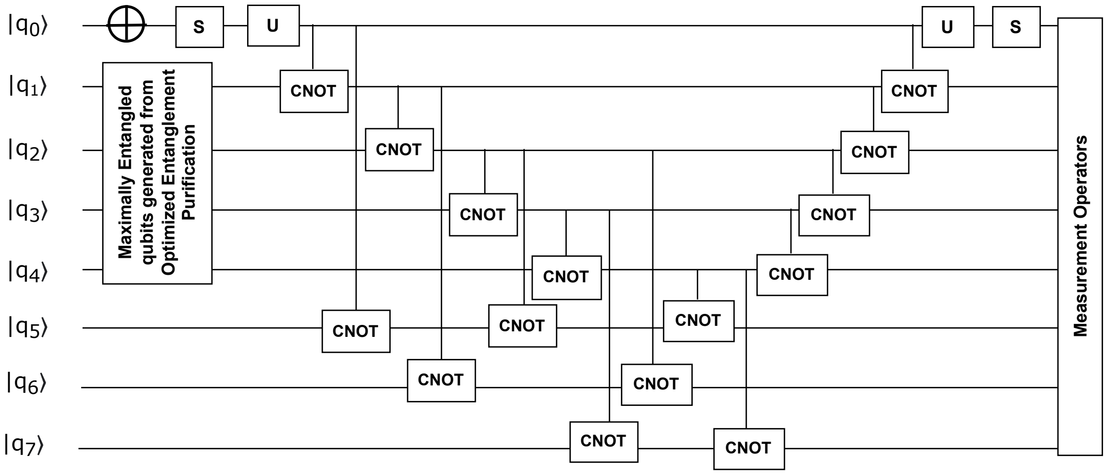

|q0⟩
|q1⟩
|q2⟩
|q3⟩
|q4⟩
|q5⟩
|q6⟩
|q7⟩
S
U
Maximally Entangled qubits generated from Optimized Entanglement Purification
CNOT
Measurement Operators

Figure 6.11: Architecture of optimized Entanglement based Quantum Error Correction

As shown in Figure 6.11, a total of five steps are performed to implement quantum error correction using entangled qubits. These are Entanglement generation, entanglement purification, encoding, syndrome measurement, and decoding. In the initial stage, entangled qubits are generated and transmitted at encoding and decoding processes. It is necessary to observe whether the qubits are maximally entangled or not in order to transmit the entangled qubits. Due to the noise and delicacy of qubits, the entanglement between qubits leads to weak entanglement. Entanglement purification techniques are performed to overcome this kind of problem. The entire cost of the error correction depends on each step. If the operations in each step are optimized, then that leads to the optimization of the final cost. Hence here we use the optimized entanglement purification technique as written in Algorithm 6.3 to generate maximal entanglement. After that, the encoding, syndrome measurement, and decoding operations are optimized as written in the following algorithm.

Algorithm 6.4 Entanglement based Asymmetric Quantum Error Correction

```
Input: Quantum Information $|\phi\rangle$
Output: Detection and correction of quantum errors in transmitted information
Initialize the number of qubits as 5
Initialize Quantum register $Q_r$, Classical register $C_r$ with size 5
Initialize Ancilla register $A_r$ with size 3
Apply Hadamard and CNOT operations on qubits
Measure the entangled pairs of state $|\psi^{\pm}_{ab}\rangle$ or $|\phi^{\pm}_{ab}\rangle$
Apply NOT operation on second and fourth qubits
Apply CNOT operations on $Q_r[0,1]$
Apply H operation on $Q_r[0], Q_r[3]$
Apply CNOT operation on $Q_r[0,3]$
Perform Bell State Measurement
Measure the information stored in Classical register $C_r[0-3]$
Find the maximally entangled pair from two entangled pairs and share those between the encoder and decoder
Apply NOT operation on initial qubit
Apply S and U operations along with X, Y and Z axis on initial
Transmit entangled qubit $|\phi^{+}_{ab}\rangle$ to second qubit
for $i = 0$ to $n-2$ do
    Perform CNOT operation on $Q_r[i]$ & $Q_r[i+1]$
end for
for $i = 0$ to $n-1$ do
    Store the information from the Quantum register to the Classical register
end for
Measure the information stored in the Classical register
$Q_r[0] \leftarrow Z$
$Q_r[0] \& A_r[0] \leftarrow$ cx
$Q_r[1] \& A_r[1] \leftarrow$ cx
$Q_r[2] \& A_r[0] \leftarrow$ cx
$Q_r[2] \& A_r[1] \leftarrow$ cx
$Q_r[3] \& A_r[2] \leftarrow$ cx
$Q_r[4] \& A_r[2] \leftarrow$ cx
$Q_r[4] \& A_r[0] \leftarrow$ cx
for $i = (n/2) + 1$ to $n-1$ do
    Store the information from the Quantum register to the Ancilla register
end for
Measure the information stored in Ancilla register
if $A_r ! = 0$ then
    Append phase gate on initial qubit
end if
for $i = 0$ to $n$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in the classical register
```

```
for $i = n - 1$ to 0 do
    Perform CNOT operation on $Q_r[i]$ & $Q_r[i-1]$
end for
$Q_r[0] \leftarrow$ Unitary operation
$Q_r[0] \leftarrow S$
$Q_r[1] \leftarrow |\phi^{+}_{ab}\rangle$
for $i = 0$ to $n - 1$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in Classical register $C_r$
```

After running the Algorithm 6.4 in quantum system, the observed results are depicted in Figure 6.12.

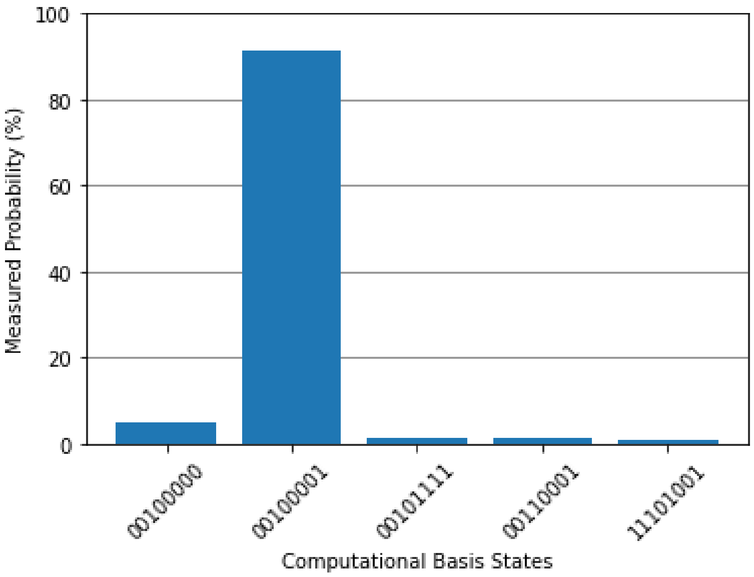


Figure 6.12: Quantum system results for optimized AQSEC using entangled Qubits

The results in Figure 6.12 shows that the fidelity of the optimized AQSEC using Entangled qubits is increased to 0.918 and error rate reduced to 8.2%

6.4 Experimental Setup

To perform the experiment, we have considered classical and quantum systems. The configuration details of the classical system are given below.

- Processor: Intel core I3
- RAM: 4GB

- Operating System: Windows 7 Ultimate

The proposed algorithm is developed and experimented on IBM Quantum System using the Qiskit tool. The configuration details of the IBM quantum system are as follows.

- System Name: ibmq_guadalupe
- Operating System: Darwin
- Tool used: Qiskit tool
- Processor: Falcon r5.11L

Along with these, we also used **RCViewer+ Tool** to measure the Quantum cost. The tool description is given below.

- Tool Name: RCViewer+ Tool
- Input file format: .tfc
- Version: Real format version 1

6.5 Result Analysis and Discussion

To implement cost-effective quantum circuits, optimized gates are crucial. In quantum computation, the quantum cost is measured based on the number of single and multi-qubit gates. One more measure to check the circuit optimization is quantum depth. Quantum depth is an integer number that represents the number of gates present in the longest path of a circuit. If the circuit is having only single input and single output gates, then the value of Quantum cost and quantum depth are almost the same. There will be a difference between quantum cost and depth values with multi-input and multi-output gates. For example, a circuit $\mathcal{C}_r$ is implemented using CNOT and Hadamard gate, then the quantum cost and quantum depth are equal i.e. 2 units. But if circuit $\mathcal{C}_r$ is implemented using Toffoli and Hadamard gates, then the quantum cost is 6 units and the Quantum depth is 2 units. Qiskit tool is used to calculate the Quantum depth. RCViewer tool is used to calculate the Quantum cost.

6.5.1 Quantum Cost Calculation using RCViewer tool

RCViewer is an analyzer and viewer tool for reversible and quantum circuits. It takes the input in .tfc (texture format cache files also called as textual input file) format. It supports NCTSF and NCT gate libraries. With this, it supports NOT, Toffoli, CNOT, Fredkin, Hadamard, Controlled V and V^+ and other reversible and quantum gates. We used the RCViewer tool to calculate the Quantum cost of the existing and optimized circuits and also to check the mathematical equivalence between existing and optimized architectures.

The detailed result analysis of the optimized entanglement purification method with the existing works in terms of quantum cost, quantum depth and gate count are depicted in Figure 6.13.

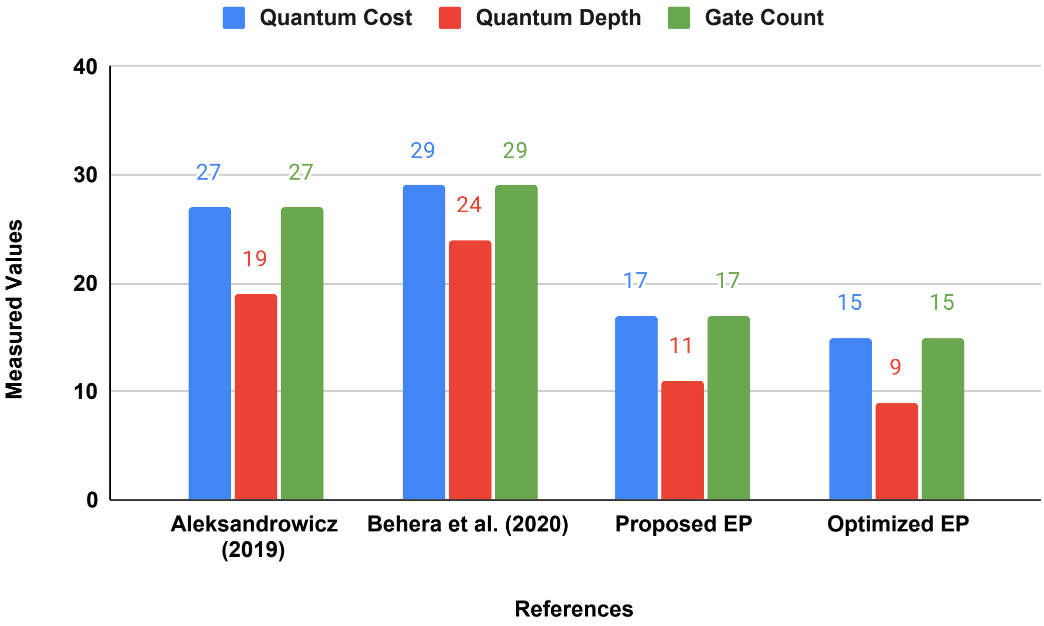


Figure 6.13: Result analysis of optimized Entanglement Purification method with existing works

From Figure 6.13, it is observed that the value of quantum cost and depth and gate count are reduced with the optimized entanglement purification method.

The optimized purification method is used to develop the optimized AQSEC using entangled qubits. The result analysis of optimized AQSEC with the existing state-of-the-art works is illustrated in Figure 6.14.

Figure 6.14 shows that the quantum cost, depth and gate count are reduced with the

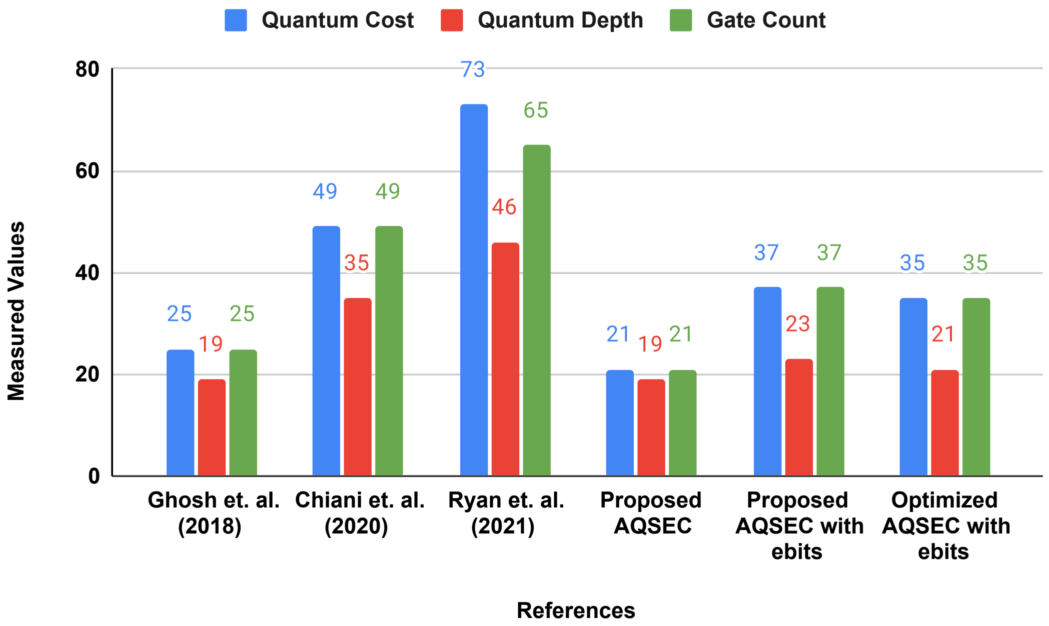


Figure 6.14: Result analysis of optimized AQEC with existing QEC models

optimized AQEC algorithm compared with the existing ones. The optimized architectures are produced efficient results with less number of quantum gates compared to the existing state-of-the-art methods.

6.6 Summary

This chapter discusses in detail the significance of Quantum cost optimization methods in present NISQ quantum systems. We also defined Quantum cost and discussed about various unit cost gates and their importance in developing optimized architectures. Further, we proposed an optimized algorithm for multi-input gates like the Toffoli gate, and Peres gate by using unit-cost reversible gates. The optimized Toffoli and Peres gates play a key role in developing reversible sequential circuits and many other applications. We also applied the cost optimization methods on the proposed entanglement purification and AQSEC methods for further optimization in terms of quantum cost, quantum depth and gate count. The proposed algorithms are developed and executed in a quantum system. The experimental results show that the proposed cost optimization algorithms of Entanglement purification and Entanglement-based Quantum Error Correction with unit cost gates optimize the existing circuits to 18% & 5.4% in terms of quantum cost and depth. The result analysis of optimized algorithms with the existing state-of-the-art methods is also demonstrated in this chapter. The optimized algorithms can be proficient in developing sequential circuits which are used in various applications like secure communication, teleportation, quantum cryptography, etc.

Chapter 7

Quantum Key Distribution

In the previous chapter, we discussed the importance of quantum cost optimization and the proposed quantum cost optimization algorithms for Entanglement Purification and Quantum Error Correction methods. The Entanglement Purification and Quantum Error Correction methods play a prominent role in various applications like Quantum Key Distribution, Quantum Repeaters, Teleportation, Secure communications, etc. To check the efficiency of the proposed Error Correction method, we have applied it in the application, i.e., Quantum Key Distribution. This chapter gives a detailed discussion of Quantum Key Distribution and Quantum Error Correction's importance in securely transmitting the key.

7.1 Significance of Quantum Error Correction in Quantum key Distribution

Quantum key distribution (QKD) is a secure communication protocol. With the existence of QKD, a new era of cryptosystems called quantum cryptography has emerged. QKD has the greatest potential to secure data from unauthorized users and possible to develop unbreakable cryptosystems. Classical cryptography, also known as symmetric-key cryptography, involves the use of a shared secret key to encrypt and decrypt messages. It is a method of secure communication that has been used for centuries and has played a significant role in the development of modern cryptography. While classical cryptography can be effective at protecting the confidentiality of messages, it is not necessarily unbreakable. In fact, many classical cryptographic methods have been broken over time as new techniques or technologies have been developed. This is because the security of any cryptographic system is dependent on the underlying assumptions and mathematical principles. As these assumptions or principles are challenged or proven to be flawed, the security of the system can be compromised. For example, in the year of 1917, Vernam (Vernam, 1926) introduced one-time pad encryption that shares a random key between the sender and receiver. When this was introduced, it was one of the effective strategies for secure data transmission. After a few decades, Shannon (Shannon, 1949) proved that the Vernam method is not optimal and there is no encryption method for the key with less size. The key shared between two parties can be breakable with high computational powers. The researchers started working on implementing cryptosystems with the largest key size so that to break these key's high-end computational powers are required. Current cryptosystems are implemented based on this strategy. With the experiments, it has been proved that the existence of a quantum system makes it easy to break the cryptosystem for which the classical computers will take some thousands of years. Most security systems in the current scenario adopt the RSA algorithm. RSA is one of the best and most highly secured algorithms. In the year of 2018, it was proved that Quantum Shor's algorithm breaks the RSA encryption in just 200 seconds whereas a supercomputer requires 10000 years to break the same (Singh Gill et al., 2020). With this, people came to know about quantum computers and how the current security systems will be in trouble. The computational power of quantum computers is exponentially high when compared to classical computers. There is a lot of scope for research in Quantum Cryptography. But it is not easy to develop new strategies for Quantum Cryptography. Quantum cryptography is entirely different when compared to classical cryptography. In classical cryptography, only classical channel is used to share the key between the sender and the receiver. In quantum cryptography, classical and quantum channels are used to share the information between two parties as shown in Figure 7.1. The key generated through the quantum particles is called quantum key. The process of sharing it between two parties through the quantum channel is called as quantum key distribution(QKD) (Sharma et al., 2021).

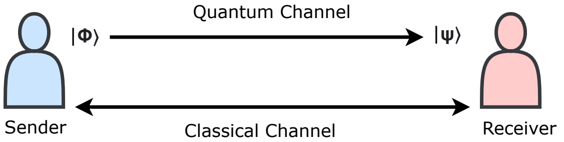


Figure 7.1: Process of Quantum key distribution

As shown in Figure 7.1, Sender generates the quantum states with polarization basis and will be sent to the receiver. The receiver uses random polarization basis to measure the quantum states sent by the sender. If the receiver uses the same basis, then the measured quantum states match with the sender's quantum states else the state changes. The matched quantum states can be considered the key and can be used in further operations. When the key has been shared, there is a possibility of an intruder who can observe the information. In a quantum system, if anyone tries to observe or measure the quantum state, then its actual state will get disturbed. Therefore the communicating parties will be able to know the third-party intervention and they can eradicate the key and restart the communication by sharing a new key.

In QKD, we observed one more case, i.e., at the receiver side even by using the same basis the key may not be the same as the sender. This is due to the noise raised from the external environment while transmitting the quantum keys. Therefore we categorized the reasons for unmatched keys even by using the same basis as follows:

- Presence of third party/eavesdropper.
- Presence of noise.

If a key is not matched due to the presence of a third party, then the communication will be restarted by sharing another key. In some cases even though it is due to the noise, the communicating parties consider it as the presence of the third party and drops that message and shares the new key. In the present era of Noisy Intermediate Scale Quantum (NISQ) Systems, the error rate is high due to the inbuilt noise of quantum particles. Noise leads to errors by adding the bit or phase flips which results in modifications of the actual quantum state and also degrades the length of the quantum key. As a solution to this, it is essential to apply quantum error correction strategies to detect and correct the errors while transmitting the quantum keys.

7.2 Proposed Methodology

As explained in the above section, to reduce the error rate and increase the efficiency of QKD, we propose two major operations. They are:

1. Maximal entanglement generation using entanglement purification method.
2. Performing error detection and correction while transmitting the quantum key.

Entangled pairs play an important role in secure data transmission. The entangled pairs used in QKD operations must be maximally entangled; otherwise leads to errors. Entanglement purification methods are required to distil maximally entangled pairs. To detect and correct the errors generated from the inbuilt noise of qubits, quantum error correction techniques need to be applied. Based on this, we propose a QKD protocol

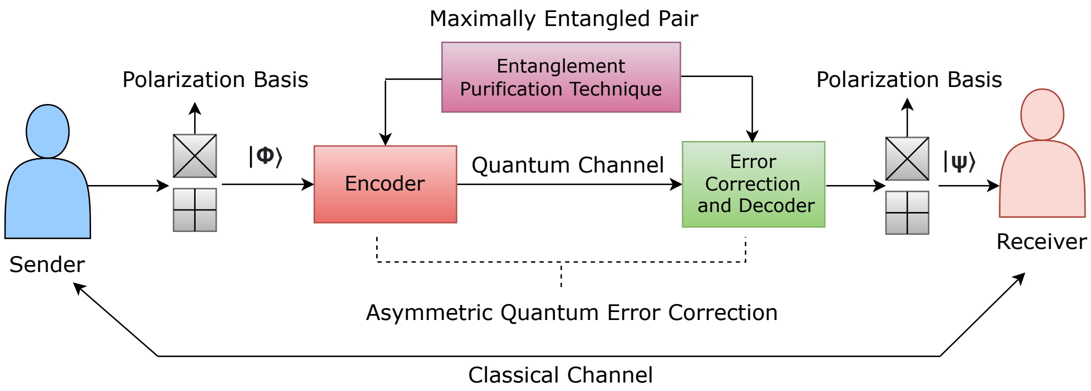


Figure 7.2: Quantum key distribution with Entanglement purification and Asymmetric Quantum Error correction

with an Entanglement purification method and Asymmetric Quantum Error Correction. The detailed architecture is depicted in Figure 7.2.

As in Figure 7.2, At first, entanglement purification is performed at the sender side to distil the maximally entangled pair from the weak ones. For that two major steps must be performed which are Entanglement generation and Entanglement Purification. A detailed discussion of these steps is presented in the following section.

7.2.1 Entanglement Generation and Entanglement Purification

Entangled pairs are represented with the help of Bell states. In a 2-level quantum system, there are a total number of four possible bell states that can be generated which are represented as follows:

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{7.1}$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{7.2}$$

After simplifying the equations for each entangled quantum state, the equations will be modified as follows:

$$|00\rangle = \frac{1}{\sqrt{2}}(|\psi^{+}\rangle + |\psi^{-}\rangle) \tag{7.3}$$

$$|01\rangle = \frac{1}{\sqrt{2}}(|\phi^{+}\rangle + |\phi^{-}\rangle) \tag{7.4}$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\phi^{+}\rangle - |\phi^{-}\rangle) \tag{7.5}$$

$$|11\rangle = \frac{1}{\sqrt{2}}(|\psi^{+}\rangle - |\psi^{-}\rangle) \tag{7.6}$$

Hadamard and CNOT gates are used to generate entanglement. To purify the generated entanglement we perform a swapping operation on entangled qubits. This method is mainly used to distil the maximally entangled pairs and to transmit the data to longer distances without interrupting the entanglement between qubits. The detailed discussion on Entanglement Purification is discussed in chapter 4. The proposed QKD experiment with entangled qubits and entanglement swapping is demonstrated as follows:

Let us consider four qubits (1,2,3,4) of two-qubit pairs (1,2)&(3,4) are entangled in same basis $|\phi^{+}\rangle$. Then the equation for $|\phi^{+}\rangle$ can be written as follows:

$$|\phi^{+}\rangle_{1234} = |\phi^{+}\rangle_{12} + |\phi^{+}\rangle_{34} \tag{7.7}$$

Above equation can be further simplified based on equation(7.2.1) as follows:

$$\begin{aligned}
|\phi^{+}\rangle_{1234} &= \frac{1}{\sqrt{2}}\left[(|01\rangle_{12} + |10\rangle_{12}) * \frac{1}{\sqrt{2}}(|01\rangle_{34} + |10\rangle_{34})\right] \\
&= \frac{1}{2}[|0101\rangle_{1234} + |0110\rangle_{1234} + |1001\rangle_{1234} + |1010\rangle_{1234}] \\
&= \frac{1}{2}[|01\rangle_{14}|10\rangle_{23} + |00\rangle_{14}|11\rangle_{23} + |11\rangle_{14}|00\rangle_{23} + |10\rangle_{14}|01\rangle_{23}]
\end{aligned}$$

The above equation further simplified by substituting the values of $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ as per the equations (3),(4),(5),(6) is as follows:

$$\begin{aligned}
|\phi^{+}\rangle_{1234} = \frac{1}{2}\Bigg[\frac{1}{\sqrt{2}}[&(|\phi^{+}\rangle_{14} + |\phi^{-}\rangle_{14})(|\phi^{+}\rangle_{23} - |\phi^{-}\rangle_{23}) \\
&+ (|\psi^{+}\rangle_{14} + |\psi^{-}\rangle_{14})(|\psi^{+}\rangle_{23} - |\psi^{-}\rangle_{23}) \\
&+ (|\psi^{+}\rangle_{14} - |\psi^{-}\rangle_{14})(|\psi^{+}\rangle_{23} + |\psi^{-}\rangle_{23}) \\
&+ (|\phi^{+}\rangle_{14} - |\phi^{-}\rangle_{14})(|\phi^{+}\rangle_{23} + |\phi^{-}\rangle_{23})]
\end{aligned}$$

After simplifying the equation through algebraic manipulations, the final equation is as follows:

$$|\phi^{+}\rangle_{1234} = \frac{1}{\sqrt{2}}\left[|\phi^{+}\rangle_{14}|\phi^{+}\rangle_{23} - |\phi^{+}\rangle_{14}|\phi^{+}\rangle_{23} + |\psi^{+}\rangle_{14}|\psi^{+}\rangle_{23} - |\psi^{+}\rangle_{14}|\psi^{+}\rangle_{23}\right]$$

The above equation shows the measurement outcomes of qubits 2 & 3 are completely random which shows the weak entanglement between qubits. Qubits 1 & 4 are correlated and highly entangled. Hence the entanglement between qubits 1,2 & 3,4 is swapped and the final maximal entangled pair resulting after the swapping is 1,4. This qubit pair is used in the proposed QKD protocol for secure key transmission. Above explained operations are performed in a quantum computer using quantum gates like Hadamard and CNOT gates as written in the following quantum algorithm.

Algorithm 7.1 Process of Entanglement purification for QKD

```
Input: Two entangled pairs
Output: Maximally entangled pair
Initialize the size of Quantum register q[] and Classical register c[] as 4
Initialize the Number of qubits n as 4
$q[1] \leftarrow X$
$q[3] \leftarrow X$
$q[0] \leftarrow H$
$q[0]$ & $q[1] \leftarrow cx$
$q[2] \leftarrow H$
$q[2]$ & $q[3] \leftarrow cx$
$q[0] \leftarrow H$
$q[2] \leftarrow H$
$q[0] \leftarrow H$
Observe the correlation between entangled pairs by performing Bell State Measurement
$q[0]$ & $q[3] \leftarrow cx$
$q[3]$ & $q[0] \leftarrow cx$
$q[0]$ & $q[3] \leftarrow cx$
$q[2] \leftarrow H$
$q[1]$ & $q[2] \leftarrow cx$
$q[2]$ & $q[1] \leftarrow cx$
$q[1]$ & $q[2] \leftarrow cx$
for i=0 to n-1 do
    $c[i] \leftarrow q[i]$   ▷ Store the information from Quantum register to Classical register
end for
for i=0 to n-1 do
    Measure c[i]   ▷ Measure the information stored in Classical register
end for
```

As written in algorithm 7.1, initially two entangled pairs are generated by performing CNOT (cx) and Hadamard operations. After generating the entanglement, entanglement swapping is performed to distil the maximally entangled pair from the two entangled pairs. Once the maximally entangled pair is generated at the sender side, that will be shared with the receiver to perform decoding operation. The quantum polarization basis is used to measure the quantum information. Usually rectilinear or diagonal basis are used to generate and measure the quantum states. Using this, the sender randomly generates the qubits and those will be encoded and sent to the receiver through the quantum channel. In between if any third party tries to measure the information with the quantum basis, then the actual quantum state will get disturbed and the modified qubit will be sent to the receiver. There are cases where the quantum states will get modified even without the interruption of a third party. That is due to the noise which is generated while transmitting the information through the quantum channel. In such cases, the error correction mechanism plays a crucial role to detect and correct the errors. To do so, the encoding, error correction, and decoding operations are performed on transmitted data to correct the errors like bit flip, phase flip, or both. We have implemented an asymmetric quantum error correction method which is represented in the following algorithm.

Algorithm 7.2 Quantum key generation steps at sender side

```
Input: Quantum Information $|\phi\rangle$
Output: Quantum key transmission in the form of encoded information
Initialize Quantum register $Q_r$, Classical register $C_r$
Initialize the Size of the key as n
Apply entanglement purification protocol (as in algorithm ??)
Generate qubits randomly using polarization basis (X or Z) with function $randint(2, size = n)$
        ▷ Sender will have the information about the basis used to generate random qubits
for i=0 to n do
    if polarization_base[i] == 0 then                ▷ Prepare qubit in Z-basis
        if qubit[i] == 0 then
            Transfer the qubit
        else
            Apply polarization basis X on $Q[0]$
            Apply polarization basis X on $Q[0]$
        end if
    else
        if qubit[i] == 0 then                        ▷ Prepare qubit in X-basis
            Apply Hadamard basis on $Q[0]$
        else
            Apply polarization basis X on $Q[0]$
            Apply Hadamard basis on $Q[0]$
        end if
    end if
end for
Apply NOT operation on initial qubit                ▷ Encoding Quantum Information
Apply S and U operations along with X, Y, and Z axis on initial
for $i = 0$ to $n - 2$ do
    Perform CNOT operation on $Q_r[i]$ & $Q_r[i+1]$
end for
for $i = 0$ to $n - 1$ do
    Store the information from the quantum register to the Classical register
end for
Measure the information stored in the classical register
Transfer the encoded information to the receiver through the quantum channel
```

As explained in the above algorithm 7.2, a single logical qubit is considered which has been generated at the sender side using a random basis. Later it will be encoded into five physical qubits to strengthen the logical qubit. This encoded data will be transmitted through the quantum channel. If any errors are detected, then those will be corrected and decoded at the receiver side using the following algorithm 7.3.

Algorithm 7.3 Quantum key generation steps at receiver side

```
Input: Encoded quantum information $|\phi\rangle$
Output: Quantum key generation
Initialize number of qubits
Initialize Quantum register $Q_r$, Classical register $C_r$
Initialize Ancilla register $A_r$
                                                    ▷ Error detection and correction
$Q_r[0] \leftarrow Z$
Perform CNOT operations on quantum states and Ancilla qubits.
for $i = 0$ to $n/3$ do
    Store the information from the quantum register to the Ancilla register
end for
Measure the information stored in ancilla register
if $A_r = 0$ then
    Q[0] ← Z
end if
for $i = 0$ to $n$ do
    Store the information from Quantum register to Classical register
end for
Measure the information stored in the classical register
```

```
for $i = n - 1$ to 0 do
    $Q_r[i]$ & $Q_r[i-1] \leftarrow CNOT$
end for
$Q_r[0] \leftarrow$ Unitary operation
$Q_r[0] \leftarrow S$
$Q_r[1] \leftarrow |\phi^{+}_{ab}\rangle$
for $i = 0$ to $n - 1$ do
    C[i] ← Q[i]
end for
Measure the information stored in Classical register $C_r$
Measure the quantum states using a random basis
if $(sender\_base[Q_i] == receiver\_base[Q_i])$ then
    Add it to an array of key bits
end if
Quantum key is generated and stored in key array    ▷ It can be used for further operations
```

Finally, the data will be measured by the receiver with the polarization basis as written in algorithm 7.3. If the receiver uses the same basis as the sender, then the data measured on the receiver side will be the same as the sent data. Once this process has been done, then the sender and receiver will discuss the basis they have used for measuring the qubit through the classical channel. The qubits which are matched with both parties can be considered as a quantum key. The result analysis of the proposed methods is discussed in the following section.

7.3 Experimental setup and Result Analysis

7.3.1 Experimental Setup

To perform the experiment, we have considered classical and quantum systems. The classical system configuration is given below

- Processor: Intel core I3
- RAM: 4GB
- Operating System: Windows 7 Ultimate

The proposed algorithm is developed and experimented on IBM Quantum System using the Qiskit tool. The configuration details of the IBM quantum system are as follows:

- System Name: ibmq_guadalupe
- Operating System: Darwin
- Tool used: Qiskit tool
- Processor: Falcon r5.11L
- Simulator Name: QASM Simulator

7.3.2 Result Analysis

The proposed QKD protocol is implemented on the IBM quantum system using the Qiskit tool. After running the algorithm 7.1 on the Quantum system, the retrieved results are depicted in the following figure.

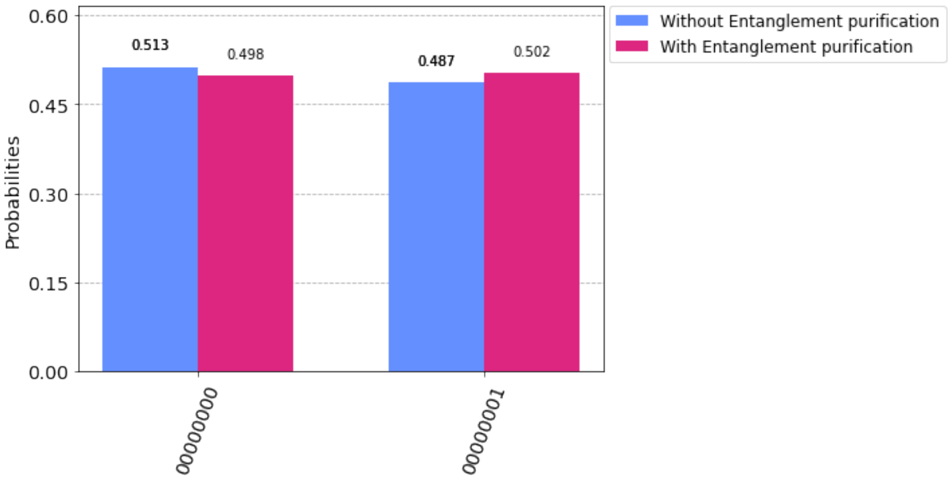


Figure 7.3: Quantum key distribution results with and without entanglement purification

Figure 7.3 shows the result analysis of the proposed entanglement purification method in QKD with the efficient result in the literature. When entangled qubits are shared between two parties, the measurement outcome of both entangled states must be 50%, i.e. 0.5. But when we implemented it in the quantum system, the measurement outcome was reduced due to the inbuilt noise. The proposed QKD protocol without entanglement purification resulting the 97.4% accuracy. Whereas, with entanglement purification, accuracy is increased to 99.6% with a reduced error rate of 0.4%, which is an efficient result compared to all the existing methods.

Even after generating the maximally entangled qubits, the quantum key length will be affected by the higher error rate of the quantum channel. The error rate has been reduced and the Quantum key length has been increased by applying the asymmetric quantum error correction in the proposed QKD protocol. We have performed experiments on a real Quantum system and Quantum simulator. The result analysis of quantum key length with the existing QKD protocol with and with Quantum Error Correction(QEC) mechanism on the Quantum system and Quantum simulator are depicted in Figure 7.4, 7.5

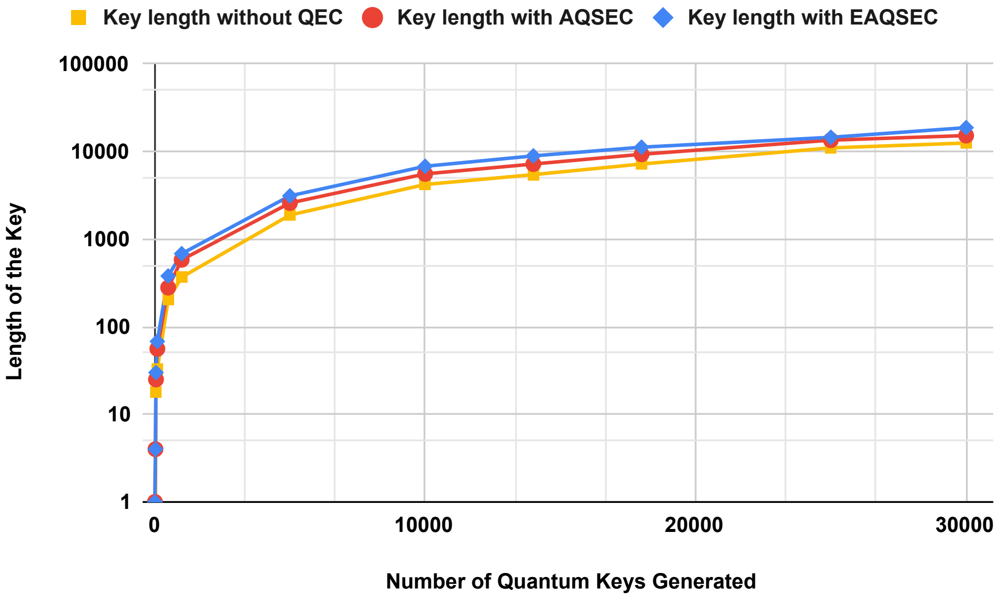


Figure 7.4: Result analysis of Quantum key length in Quantum System

Figures 7.4, 7.5 shows that the key length has improved by applying Quantum error correction along with QKD protocol. With the increasing number of qubits, the key length also increases by around 25%. As a result, QKD's communication efficiency also improved compared to the existing QKD protocols.

7.3.3 Calculation of QKD communication efficiency

Cabello (Cabello, 2000) has proposed an equation for calculating communication efficiency as follows:

$$\rho = \frac{E_n}{C_b + T_b} \tag{7.8}$$

Where E_n is the expected number of secret keys obtained by the sender/receiver, T_b

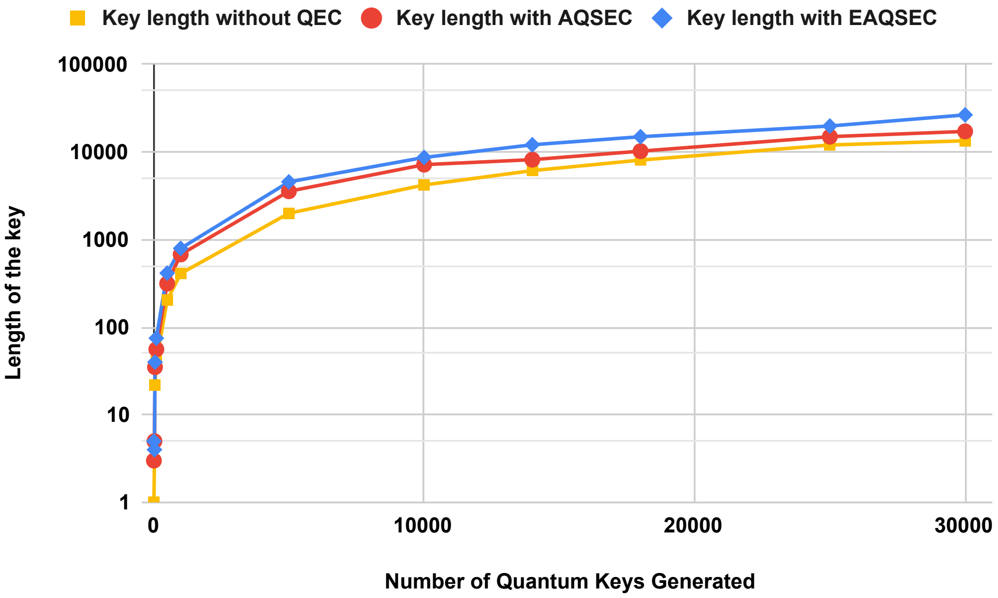


Figure 7.5: Result analysis of Quantum key length in quantum Simulator

represents the number of qubits transmitted and C_b represents the number of classical bits sent (if any). According to this, we have analyzed the communication efficiency of the proposed protocol with existing ones. The result analysis table is given as follows.

The analysis of the communication efficiency of proposed and existing QKD protocols have been shown in Table 7.1. We compared our results with the existing state-of-the-art works Song (2004); Li et al. (2018); Qin et al. (2021); Wen-Zhao et al. (2022) and many others. The authors used different methods like Bell state Preparation (BSP), Random Number Generator (RNG) and QKD as represented in Table 7.1 to transmit the data from one end to another. From the results, it has been observed that the proposed protocol improves communication efficiency compared to the existing state-of-the-art techniques. In most of the existing papers, researchers have concentrated on improving the quantum key rate and key length. But while doing that, the parameters like the number of classical bits, and quantum generated and transmitted bits using QKD affects the communication efficiency. But the proposed protocol was implemented by considering all the points to improve efficiency and the quantum key length. The error rate analysis is depicted in the following Figure 7.6.

Table 7.1: Analysis of QKD Communication Efficiency

S.No	QKD Protocol	Method Used	Efficiency(ρ)
1	Song (2004)	BSP	0.5
2	Guo et al. (2006)	BSP	0.58
3	Gao (2008)	BSP	0.67
4	Dong & Teng (2010)	QKD	0.61
5	Shalm et al. (2015)	BSP	0.7515
6	Giustina et al. (2015)	BSP	0.774
7	Liu et al. (2018)	RNG	0.794
8	Bierhorst et al. (2018)	RNG	0.755
9	Li et al. (2018)	BSP	0.7875
10	Zhang et al. (2020)	RNG	0.76
11	Zhang & Zheng (2021)	BSP	0.78
12	Qin et al. (2021)	BSP	0.71
13	Shalm et al. (2021)	RNG	0.763
14	Liu et al. (2021)	RNG	0.8135
15	Wen-Zhao et al. (2022)	QKD	0.8749
16	**Proposed Method**	**QKD**	**0.892**

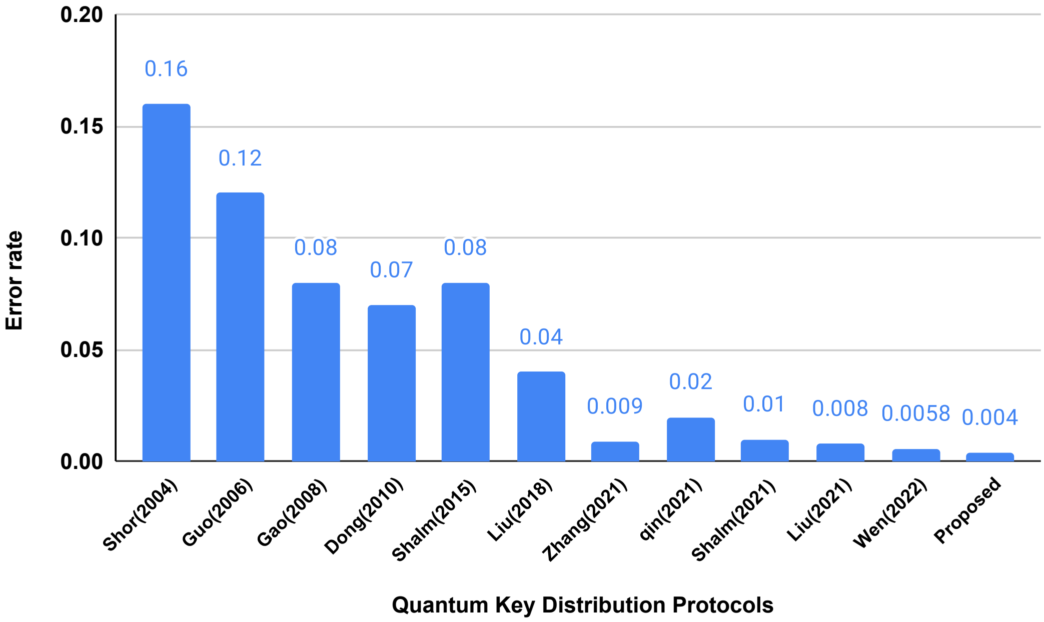


Figure 7.6: Analysis of Error rate

7.4 Third party Risk Analysis

It is also important to analyze the risk of third-party interference. For instance, consider Figure 7.7 which shows the third-party interference in key distribution from sender to receiver. The third-party risk analysis in secure quantum communication is depicted in Figure 7.8.

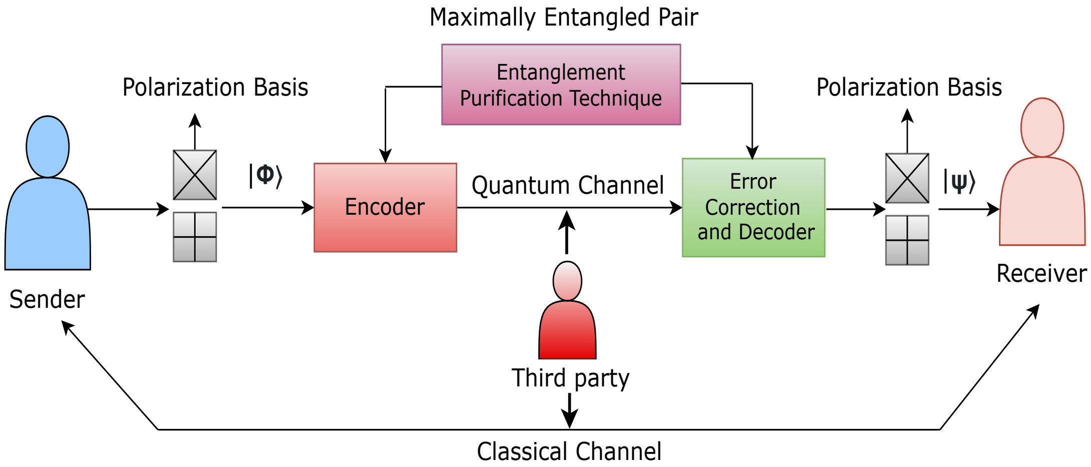


Figure 7.7: Third party Interference in QKD

As shown in Figure 7.7, if any third person tries to observe the information transmitted between sender and receiver, then the possibility of him/her detecting the key is depicted in Figure 7.8.

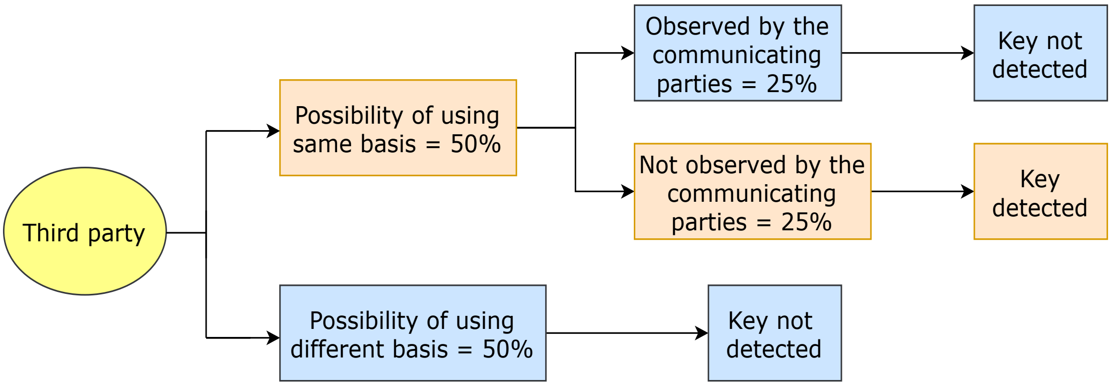

Third party
Possibility of using same basis = 50%
Observed by the communicating parties = 25%
Key not detected
Not observed by the communicating parties = 25%
Key detected
Possibility of using different basis = 50%
Key not detected

Figure 7.8: Third party risk analysis

Figure 7.8 represents the probability of detecting a key when a single qubit is transmitted from the sender to the receiver. According to this, 25% (i.e. 0.25) possibility is there for a third person to detect the key. If the Quantum communication is made up of 2 qubits, then the probability of detecting the key will be $0.25 * 0.25 = 0.0625$. This is very less compared to the single qubit transmission. For n-qubits, the equation can be modified as 0.25^n. If we consider 10 qubits for transmission, the third-party key detection probability will be negligible.

7.4.1 Third party detection rate

Even though the possibility of detecting the key is very negligible with more number of qubits, it is important to find the third-party intervention. If any third party measures the information before the receiver receives it, then it is crucial to detect his/her intervention by the sender and receiver. In the case of single qubit transmission, the probability of detecting the third-party intervention can be calculated by considering the following cases:

1. The possibility of a third party using the same basis as sender and receiver is 50%. In such cases, the third party may not be detected.
2. The possibility of a third party using a different basis than the sender and receiver is 50%. In such cases, the detection of the third party depends on the receiver's measurement.
    (a) If the receiver uses the same basis as the sender then the possibility of detecting third-party intervention is 25%
    (b) If the receiver uses a different basis than the sender, the third party goes undetected. The possibility to happen this is 25%

From all the above-mentioned points, it is clear that the total probability of third-party detection is 75%. This is in the case of single qubit transmission. If 2 qubits are transmitted, the probability of third-party detection is $75\% * 75\% = 0.75 * 0.75 = 0.5625$. Similarly, for n-qubits, the formula will be modified as 0.75^n. For n=10, the probability of third-party detection is 0.05 which is very negligible. Therefore the proposed quantum key distribution protocol provides higher security with a reduced third-party detection rate and quantum key detection rate by using a minimum of 10 qubits. If more than 10 qubits are used for QKD, then the security levels will be high compared to the existing key distribution strategies.

7.5 Summary

This chapter discussed the Quantum Key distribution protocol using Entanglement Purification and Quantum Error Correction strategies. Two algorithms were proposed for Sender side key generation and key finalization at the receiver side along with the entanglement purification algorithm (discussed in Chapter 4) in order to perform QKD. The proposed algorithms improve the quantum key length and communication efficiency compared to the existing works. It also reduces the third-party error detection rate. The proposed algorithms are developed and executed on the IBM Quantum Computer using the Qiskit tool. The conclusions and future work of the proposed methods are described in the next chapter.

Chapter 8

Conclusion and Future Work

Quantum Error Correction(QEC) plays a key role in fault-tolerant quantum computation in order to reduce the effects of quantum noise on quantum gates, quantum circuits, stored information, and measurements. In classical computation, error correction operations are performed by adding redundancies to the computation. An example of this is classical repetition code. It is not possible to add redundancy in quantum computation as per the no-cloning theorem. Quantum Error Correction(QEC) methods are introduced to solve the issue of redundancy. In QEC, quantum encoders will be used to convert a single logical qubit into multiple physical qubits. With this, it is possible to detect and correct errors. There are various methods to perform QEC. Most of the QEC methods are symmetric. The research work in this thesis is directed towards the design and development of the Asymmetric Quantum Syndrome Error Correction(AQSEC) using Entangled qubits.

We proposed an Entanglement purification (EP) algorithm to distil the maximally entangled pairs from weak ones for the development of AQSEC using entangled qubits. Entanglement generation and Entanglement swapping operations were performed to develop the EP method. These operations are performed using Controlled-NOT and Hadamard gates and Measurement operations. The proposed method is developed and experimented on a Quantum system and Quantum simulator. The fidelity of the maximally entangled pairs in the Quantum system is 0.871 with an error rate of 0.129. From the Quantum simulator results, it is observed that the fidelity of the maximally entangled pair is 0.9926. Simulator results are affected due to the sampling error. From the Quantum system and simulator results, it has been observed that the proposed EP method outperforms the existing methods. The next step is to develop Asymmetric Quantum Syndrome Error Correction. The proposed AQSEC method performs encoding, error detection, correction, and decoding operations. Encoding operation is an initial and important step in AQSEC. It encodes the single logical qubit into multiple physical qubits. In the proposed algorithm, Phase, Unitary, and Controlled NOT operations are performed to encode the quantum information and to strengthen the data from phase flip errors. The encoded information is transmitted through the quantum channel.

To avoid data loss, depolarizing quantum channel is considered for data transmission. Whenever the data is transmitted through the quantum channel, there is a possibility of getting bit flip, phase flip, or both bit and phase flip errors. A syndrome measurement algorithm is developed to detect the type of error and exactly on which physical qubit it has occurred along with the error correction process. An algorithm is developed to decode the encoded information to know the original(logical) quantum state once the error is corrected. From the experimental results, it is observed that the fidelity of the proposed AQSEC is 0.8589. The entanglement is added to the AQSEC in order to improve fidelity. The maximally entangled pair is shared at encoding and decoding operations. By adding these qubits, it is observed that the final results were more efficient than the proposed AQSEC algorithm. The AQSEC with entangled qubits achieved 0.905 fidelity. The proposed AQSEC using entangled qubits has also experimented on a Quantum simulator. The achieved fidelity of the proposed algorithm in the simulator is 0.9896.

After developing new architectures, it is necessary to examine whether the architectures are optimized in terms of quantum cost and depth. Quantum cost optimization models are developed for proposed Entanglement purification and AQSEC algorithms to address this. A circuit's quantum cost and depth are optimized by replacing the higher-cost quantum gates with lower-cost gates. The proposed quantum cost optimization methods for the Toffoli gate, Peres gate, Entanglement purification and Entanglement-based Quantum Error Correction with unit cost gates optimize the existing circuits by 20% in terms of quantum cost, quantum depth and gate count. Finally, the proposed AQSEC using entangled qubits is used to develop a Quantum key distribution(QKD) protocol. Quantum key distribution plays a key role in secure data transmission. In the proposed QKD protocol, three operations are performed. These are entanglement purification, Sender side key generation and key finalization at the receiver side. It has been observed that the proposed QKD outperforms the existing QKD protocols in terms of communication efficiency with a reduced third-party key detection rate based on the experimental results.

All the proposed algorithms are developed and executed on the IBM Quantum Computer using the Qiskit tool. RCViewer tool is used to calculate the quantum cost. From the experimental results, it is observed that the proposed entanglement Purification, AQSEC, Quantum cost optimization method, and QKD protocol outperform the state-of-the-art methods. Improvement of the proposed methods can be considered in the future research directions.

- The proposed Error correction methods can be improvised to perform fault tolerance quantum computation with the longest period of data storage facilities.
- Once the quantum systems are made available, then the proposed AQSEC can be experimented using less number of qubits to achieve better performance and to reduce the error rate.
- The proposed AQSEC method can be extended to reduce the inbuilt noise in the Quantum states.
- Asymmetric quantum syndrome error correction method can be further improvised by adding the ability to correct a large number of errors, as this would enable more reliable quantum information processing and communication.
- The proposed AQSEC can be applied in various applications like drug design, repeaters, longer-distance data transmission, etc.

Appendix-A

Experimental Analysis of a Quantum Encoder in Various Quantum Systems

Quantum computer performs operations by adopting the principles of quantum physics and quantum mechanics. With these principles, it performs operations exponentially faster compared to classical computers. The major problem observed in quantum computation is noise and decoherence. The noise and decoherence generate errors while performing the operations on quantum states. As a solution to this, Quantum error correction(QEC) methods are introduced. Encoding plays a key role in QEC. In the encoding process, the logical qubits are encoded into physical qubits by appending extra qubits to them. With this, the logical qubit will be strengthened and can be transferred safely. Initially, the experimental results of quantum computation are theoretical or mathematical. But with the existence of quantum computers, it is possible to develop and run new quantum architectures on publicly available quantum computers. Thus, we developed an efficient algorithm for encoding quantum information using various quantum gates. The developed algorithm is executed on various quantum systems and the performance is analyzed in terms of frequency, run time, error rate, number of qubits, and quantum volume. This analysis helps the researchers to opt an efficient quantum system to perform the experiments.

A.1 Proposed Encoder and its implementation in Quantum systems

In QEC, encoding plays a vital role in transmitting quantum information safely. Quantum encoding is a process of encoding a single logical qubit into multiple physical qubits to strengthen the actual quantum state. The extra qubits are added to the logical qubit in this stage. If we will perform efficient operations to encode the information then it leads to fewer errors. While implementing the new architecture for encoding, we can perform the error reduction procedure prior. With this, we can strengthen the quantum state and prevent errors. Even if the error occurs then those can be detected easily with this process. In the proposed method, initially, we have considered a single logical qubit that will be encoded into 5 physical qubits. The step-by-step procedure for implementing the quantum encoder is represented in Algorithm 5.1 in Chapter 5.

As written in algorithm 5.1, initially a single logical state $|1\rangle$ is taken as an input. To encode it into 5 physical qubits, Phase(S), Unitary and CNOT operations are performed. S and Unitary operations are performed on single input and single output gates. These operations are used to rotate the quantum state along with the X, Y, and Z axis. CNOT is a two-input and two-output gate. It is implemented with Not and XOR operations. With S, Unitary, and CNOT operations it is easy to detect the bit and phase flip errors. After performing S and Unitary operations, CNOT operations will be applied on quantum states to convert a single logical qubit into multiple physical qubits. After performing these operations, the resulted outcome with input state $|1\rangle$ is $|11111\rangle$. The proposed algorithm is developed and experimented in various quantum systems using the Qiskit tool. After running this algorithm on various IBM quantum systems named Quito, Lima, Belem, Bogota, Manila, Jakarta, and Perth the retrieved results are depicted in the figures A1, A2, A3, A4, A5, A6, A7.

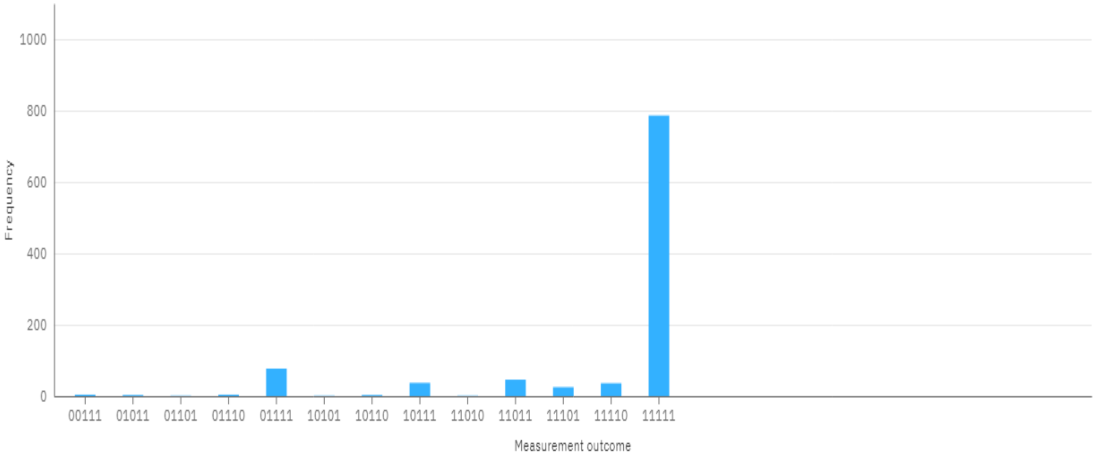


Figure A1: Encoder results on system ibmq_quito

Figure A1 represents the quantum results of the proposed encoder in the Quito system. It is a 5-qubit system with a volume of 16. The output frequency of the proposed encoder in the Quito system is 786 out of 1000 cycles. Quantum volume represents the largest circuit a quantum system can implement successfully. i.e., Quito can implement a quantum circuit with size 16 and can run it.

Figure A2 represents the quantum results of the proposed encoder in the Lima system. It is a 5-qubit system with volume 8. The output frequency of the proposed encoder in the Lima system is 735.

Figure A3 represents the quantum results of the proposed encoder in the Belem sys-

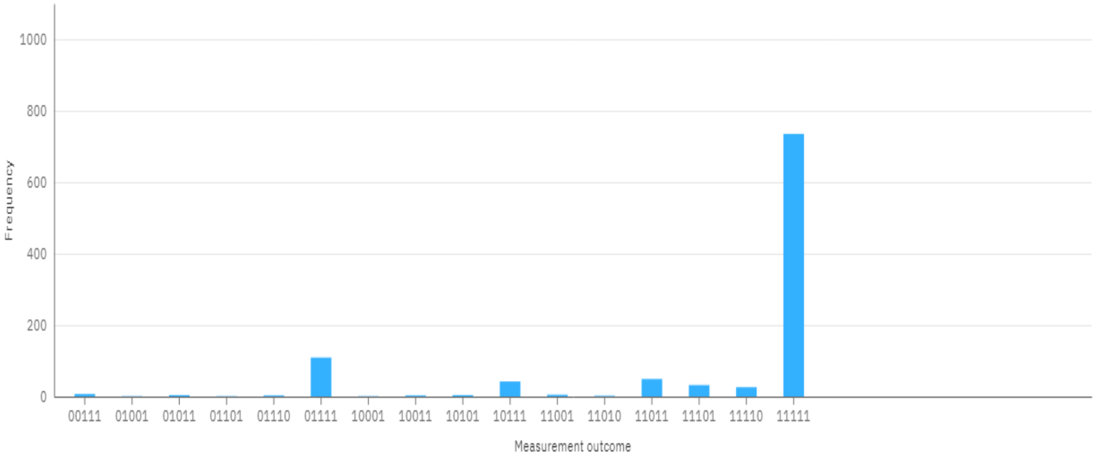


Figure A2: Encoder results on system ibmq_lima

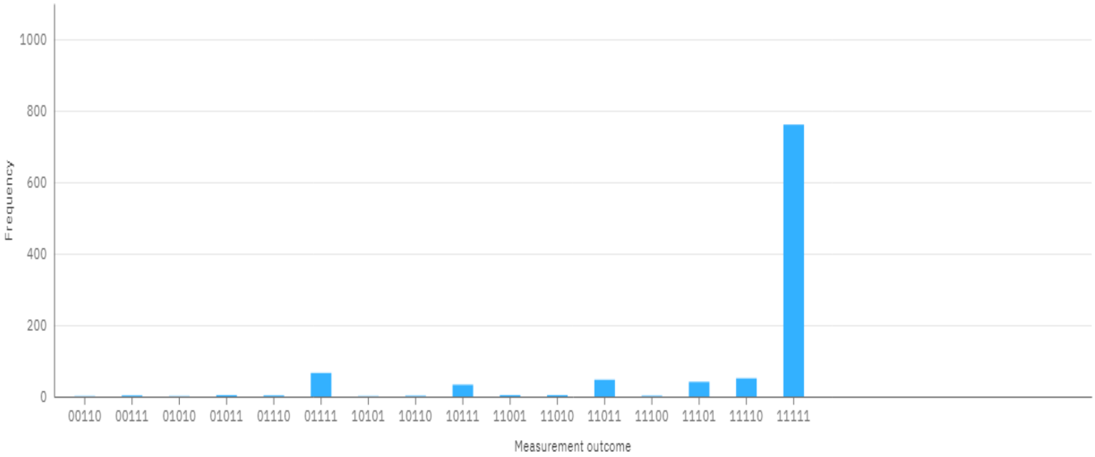


Figure A3: Encoder results on system ibmq_belem

tem. It is a 5-qubit system with a volume of 16. The output frequency of the proposed encoder in the Belem system is 761.

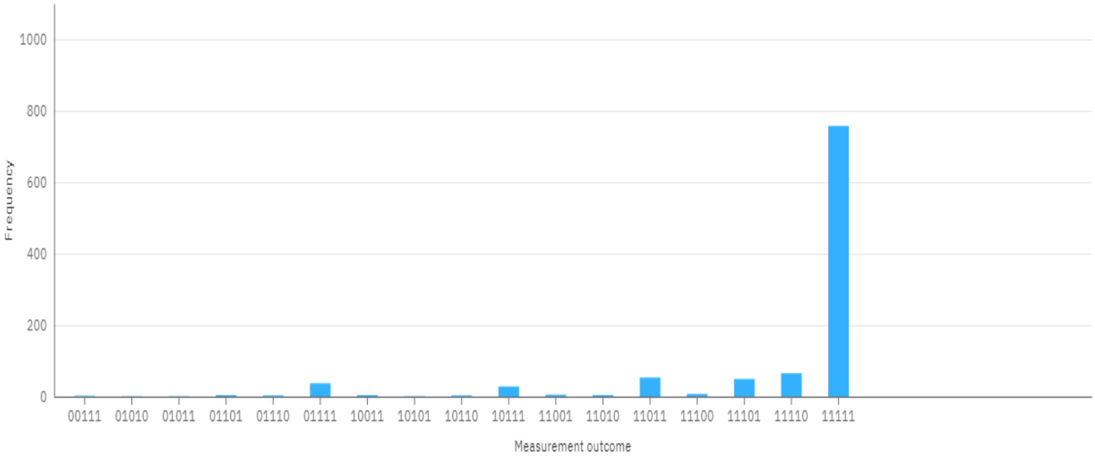


Figure A4: Encoder results on system ibmq_bogota

Figure A4 represents the quantum results of the proposed encoder in the Bogota system. It is a 5-qubit system with a volume of 32. The output frequency of the proposed encoder in the Bogota system is 757.

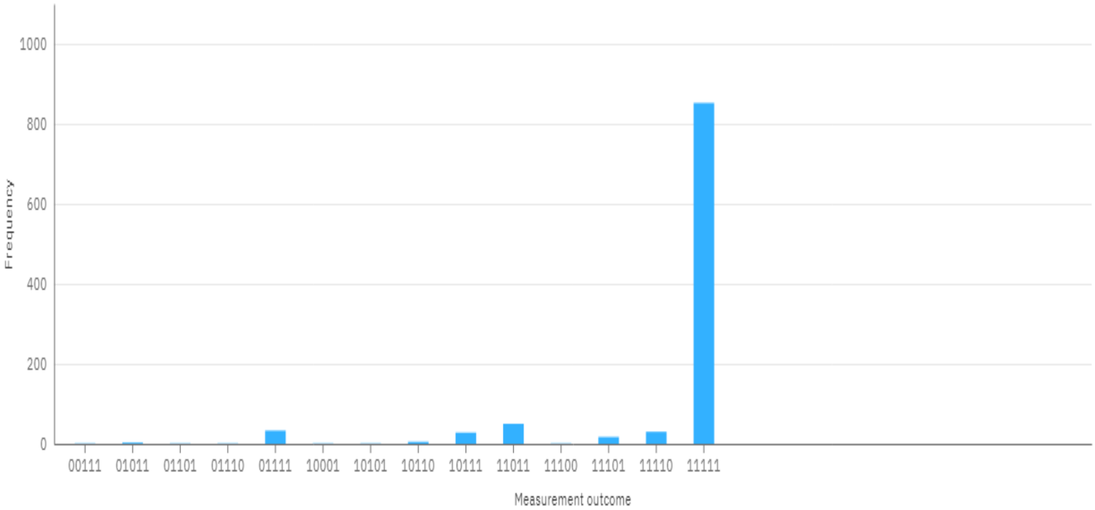


Figure A5: Encoder results on system ibmq_manila

Figure A5 represents the quantum results of the proposed encoder in the Manila system. It is a 5-qubit system with a volume of 32. The output frequency of the proposed encoder in the Manila system is 852.

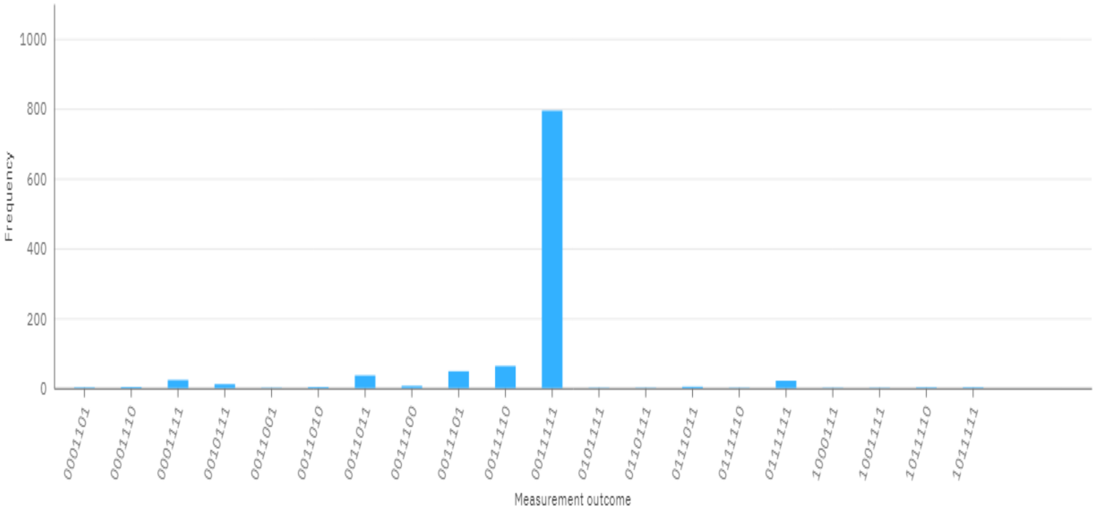


Figure A6: Encoder results on system ibmq_jakarta

Figure A6 represents the quantum results of the proposed encoder in the Jakarta system. It is a 7-qubit system with a volume of 16. The output frequency of the proposed encoder in the Jakarta system is 794.

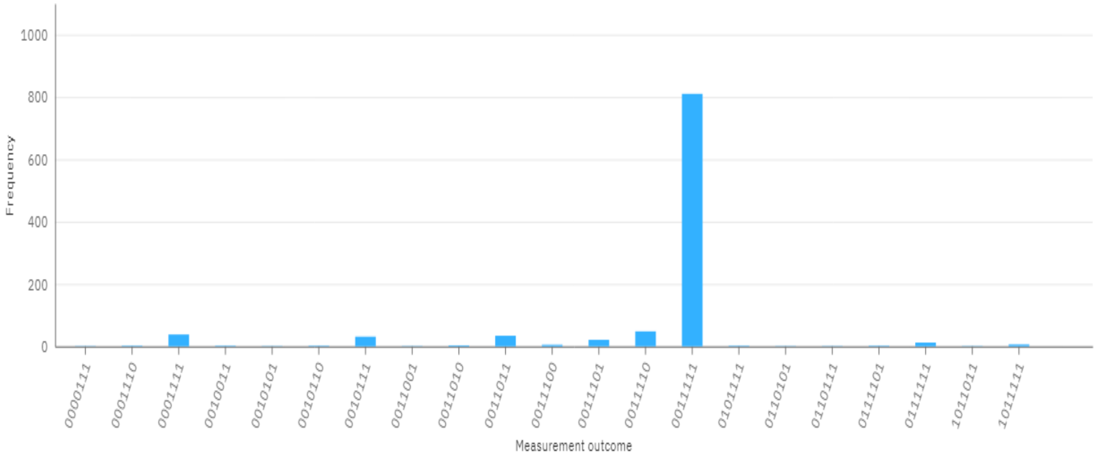


Figure A7: Encoder results on system ibm_perth

Figure A7 represents the quantum results of the proposed encoder in the Perth system. It is a 7-qubit system with a volume of 32. The output frequency of the proposed encoder in the Jakarta system is 810.

The analysis of all the above-mentioned quantum systems results in terms of the number of qubits, run time, frequency of getting expected output, and the average error rate are discussed in the following section.

A.2 Result analysis of various Quantum systems

The proposed encoder algorithm is implemented and executed on IBM Quantum experience(QE). It is a quantum platform and provides cloud access to its quantum computers. It helps researchers to perform experiments on real-time quantum systems. It provides public access to 5 and 7-qubit quantum systems, on which we can perform the experiments. All these systems are designed with different quantum volumes. Quantum volume represents the largest circuit a quantum system can implement successfully. It also represents the maximum number of CLOPS i.e., the maximum number of circuit operations performed on a quantum computer. The detailed analysis of each system with obtained results is represented in Table A1.

From Table A1, it is observed that the 5-qubit system Manila gives an efficient result due to the less error rate and high quantum volume. Lima gives inefficient results due to the high error rate and lower quantum volume. It is observed that to perform 5-qubit experiments Manila will be a better choice. For 7-qubit operations, Perth gives efficient results with less error rate and high quantum volume. The number of qubits

Table A1: Comparison of results with various quantum systems

Name of the system	**No.of Qubits**	**Run time**	**Average Assignment error**	**Output Frequency**	**Quantum Volume**
Quito	5	4.1s	$2.598e^{-2}$	786	16
Lima	5	4.4s	$4.164e^{-2}$	735	8
Belem	5	3.9s	$2.852e^{-2}$	761	16
Bogota	5	7.1s	$3.982e^{-2}$	757	32
Manila	5	5.7s	$2.562e^{-2}$	852	32
Jakarta	7	6.1s	$3.354e^{-2}$	794	16
Perth	7	3.5s	$2.906e^{-2}$	810	32

and quantum volume also affect the run time. The analysis between these three are depicted in the following Figure A8.

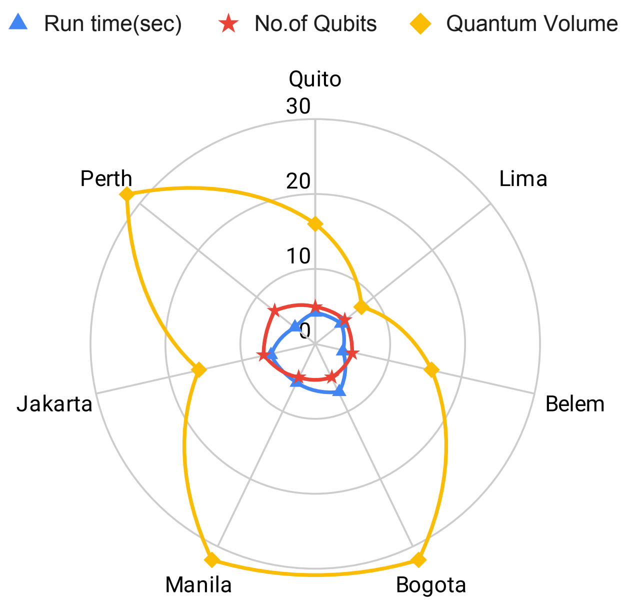


Figure A8: Analysis between Number of qubits, Quantum Volume and Program Run time.

At present, the research in quantum computing has increased because of its exponential computational power. With this many researchers are performing experiments on quantum systems to develop applications in various fields. In such instances, the analysis of various systems will help the researchers to opt an efficient system to perform the experiments.

A.3 Summary

The implementation and the result analysis of a quantum encoding method on various quantum systems have been discussed in this chapter. Encoding plays an important role in Quantum Error Correction. The proposed encoding method can be beneficial in implementing an efficient QEC model to detect and correct errors. The proposed algorithm is executed on various quantum systems and the retrieved results are analyzed to find an efficient quantum system to perform operations.

From the results. it has been observed that the noise increases with the increasing number of qubits. We performed the experiment on 5-qubit and 7-qubit quantum computers. The result mainly depends on the quantum volume and the number of circuit operations performed per second. These are specified in the processor structure of each quantum system. Based on this the results are affected even though the operations performed are the same. Finally from the results, it is observed that the proposed encoding method performs well and gives an efficient result in the 5-qubit system Manila with the highest frequency of 852.

References

Ahsan, M. & Naqvi, S. A. Z. (2020). Reconfiguring quantum error-correcting codes for real-life errors. *Journal of Physics D: Applied Physics*, *53*(41), 415302.

Aleksandrowicz, Gadi, e. a. (2019). Qiskit: An open-source framework for quantum computing. *Zenodo*.

Ali, M. B., Hirayama, T., Yamanaka, K., & Nishitani, Y. (2015). Quantum cost reduction of reversible circuits using new toffoli decomposition techniques. In *2015 International Conference on Computational Science and Computational Intelligence (CSCI)*, 59–64. IEEE.

Allahmadi, A., AlKenani, A., Hijazi, R., Muthana, N., Özbudak, F., & Solé, P. (2022). New constructions of entanglement-assisted quantum codes. *Cryptography and Communications*, *14*(1), 15–37.

Aly, S. A. (2008). Asymmetric quantum bch codes. In *2008 International Conference on Computer Engineering & Systems*, 157–162. IEEE.

Aly, S. A., Klappenecker, A., & Sarvepalli, P. K. (2007). On quantum and classical bch codes. *IEEE Transactions on Information Theory*, *53*(3), 1183–1188.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G., Buell, D. A., et al. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510.

Azad, U., Lipińska, A., Mahato, S., Sachdeva, R., Bhoumik, D., & Majumdar, R. (2021). Surface code design for asymmetric error channels. *IET Quantum Communication*.

Babar, Z., Chandra, D., Nguyen, H. V., Botsinis, P., Alanis, D., Ng, S. X., & Hanzo, L. (2018). Duality of quantum and classical error correction codes: Design principles and examples. *IEEE Communications Surveys & Tutorials*, *21*(1), 970–1010.

Ball, S. & Puig, P. (2021). The geometry of non-additive stabiliser codes. *arXiv preprint arXiv:2107.11281*.

Banerjee, A. (2010). Reversible cryptographic hardware with optimized quantum cost and delay. In *2010 Annual IEEE India Conference (INDICON)*, 1–4. IEEE.

Banerjee, A. & Pathak, A. (2009). An algorithm for minimization of quantum cost. *arXiv preprint arXiv:0910.2129*.

Barabasi, S., Barrera, J., Bhalani, P., Dalvi, P., Dimiecik, R., Leider, A., Mondrosch, J., Peterson, K., Sawant, N., & Tappert, C. C. (2019). Student user experience with the ibm qiskit quantum computing interface. In *Future of Information and Communication Conference*, 547–563. Springer.

Basak, A., Sadhu, A., Das, K., & Sharma, K. K. (2019). Cost optimization technique for quantum circuits. *International Journal of Theoretical Physics*, *58*(9), 3158–3179.

Behera, B. K., Seth, S., Das, A., & Panigrahi, P. K. (2019). Demonstration of entanglement purification and swapping protocol to design quantum repeater in ibm quantum computer. *Quantum Information Processing*, *18*(4), 1–13.

Benioff, P. (1982). Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, *29*(3), 515–546.

Bennett, C. H. (1973). Logical reversibility of computation. *IBM journal of Research and Development*, *17*(6), 525–532.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical review letters*, *68*(21), 3121.

Bennett, C. H. & Brassard, G. (1984). An update on quantum cryptography. In *Workshop on the theory and application of cryptographic techniques*, 475–480. Springer.

Bhoumik, D., Sen, P., Majumdar, R., Sur-Kolay, S., Iyengar, S. S., et al. (2021). Efficient decoding of surface code syndromes for error correction in quantum computing. *arXiv preprint arXiv:2110.10896*.

Bierhorst, P., Knill, E., Glancy, S., Zhang, Y., Mink, A., Jordan, S., Rommal, A., Liu, Y.-K., Christensen, B., Nam, S. W., et al. (2018). Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, *556*(7700), 223–226.

Bloch, F. (1946). Nuclear induction. *Physical review*, *70*(7-8), 460.

Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., & Zeilinger, A. (1997). Experimental quantum teleportation. *Nature*, *390*(6660), 575–579.

Brun, T., Devetak, I., & Hsieh, M.-H. (2006). Correcting quantum errors with entanglement. *science*, *314*(5798), 436–439.

Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, *81*(14), 3018.

Cabello, A. (2000). Quantum key distribution in the holevo limit. *Physical Review Letters*, *85*(26), 5635.

Cai, W., Ma, Y., Wang, W., Zou, C.-L., & Sun, L. (2021). Bosonic quantum error correction codes in superconducting quantum circuits. *Fundamental Research*, *1*(1), 50–67.

Calderbank, A. R. & Shor, P. W. (1996). Good quantum error-correcting codes exist. *Physical Review A*, *54*(2), 1098.

Cane, R., Chandra, D., Ng, S. X., & Hanzo, L. (2020). Mitigation of decoherence-induced quantum-bit errors and quantum-gate errors using steane's code. *IEEE Access*, *8*, 83693–83709.

Cao, C., Zhang, C., Wu, Z., Grassl, M., & Zeng, B. (2022). Quantum variational learning for quantum error-correcting codes. *arXiv preprint arXiv:2204.03560*.

Caves, C. M. (1999). Quantum error correction and reversible operations. *Journal of Superconductivity*, *12*(6), 707–718.

Chandra, D., Babar, Z., Nguyen, H. V., Alanis, D., Botsinis, P., Ng, S. X., & Hanzo, L. (2017). Quantum topological error correction codes: The classical-to-quantum isomorphism perspective. *IEEE Access*, *6*, 13729–13757.

Chen, H. (2022). Mds entanglement-assisted quantum codes of arbitrary lengths and arbitrary distances. *arXiv preprint arXiv:2207.08093*.

Chiani, M. & Valentini, L. (2020a). Short codes for quantum channels with one prevalent pauli error type. *IEEE Journal on Selected Areas in Information Theory*, *1*(2), 480–486.

Chiani, M. & Valentini, L. (2020b). Short codes for quantum channels with one prevalent pauli error type. *IEEE Journal on Selected Areas in Information Theory*, *1*(2), 480–486.

Chiaverini, J., Leibfried, D., Schaetz, T., Barrett, M. D., Blakestad, R., Britton, J., Itano, W. M., Jost, J. D., Knill, E., Langer, C., et al. (2004). Realization of quantum error correction. *Nature*, *432*(7017), 602–605.

Church, A. C.-C. (2003). Classical physics and the church–turing thesis. *Journal of the ACM (JACM)*, *50*(1), 100–105.

Chuu, C.-S., Cheng, C.-Y., Wu, C.-H., Wei, C.-Y., Huang, S.-Y., Chen, Y.-J., Feng, S.-W., & Yang, C.-Y. (2021). Purification of single and entangled photons by wavepacket shaping. *Advanced Quantum Technologies*, *4*(3), 2000122.

Cleve, R. (1997). Quantum stabilizer codes and classical linear codes. *Physical Review A*, *55*(6), 4054.

Convy, I., Liao, H., Zhang, S., Patel, S., Livingston, W. P., Nguyen, H. N., Siddiqi, I., & Whaley, K. B. (2022). Machine learning for continuous quantum error correction on superconducting qubits. *New Journal of Physics*, *24*(6), 063019.

Criger, B., Moussa, O., & Laflamme, R. (2012). Quantum error correction with mixed ancilla qubits. *Physical Review A*, *85*(4), 044302.

Cuvelier, T. C., Lanham, S. A., La Cour, B. R., & Heath, R. W. (2021). Quantum codes in classical communication: A space-time block code from quantum error correction. *IEEE Open Journal of the Communications Society*, *2*, 2383–2412.

Das, P., Locharla, A., & Jones, C. (2022). Lilliput: a lightweight low-latency lookup-table decoder for near-term quantum error correction. In *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, 541–553.

De Ronde, C. (2018). Quantum superpositions and the representation of physical reality beyond measurement outcomes and mathematical structures. *Foundations of Science*, *23*(4), 621–648.

Delfosse, N., Reichardt, B. W., & Svore, K. M. (2021). Beyond single-shot fault-tolerant quantum error correction. *IEEE Transactions on Information Theory*, *68*(1), 287–301.

Donald, J. & Jha, N. K. (2008). Reversible logic synthesis with fredkin and peres gates. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, *4*(1), 1–19.

Dong, J. & Teng, J. (2010). Quantum key distribution protocol of mesh network structure based on n+ 1 epr pairs. *Journal of Systems Engineering and Electronics*, *21*(2), 334–338.

Dušek, M., Lütkenhaus, N., & Hendrych, M. (2006). Quantum cryptography. *Progress in Optics*, *49*, 381–454.

Ebison, M. (1985), The historical development of quantum theory volume 1 parts 1 and 2: The quantum theory of planck, einstein, bohr and sommerfeld–its foundation and the rise of its difficulties 1900–1925.

Ecker, S., Sohr, P., Bulla, L., Ursin, R., & Bohmann, M. (2022). Remotely establishing polarization entanglement over noisy polarization channels. *Physical Review Applied*, *17*(3), 034009.

Ekert, A. K. (1992). Quantum cryptography and bell's theorem. In *Quantum Measurements in Optics* 413–418. Springer.

Ezerman, M. F., Jitman, S., Kiah, H. M., & Ling, S. (2013). Pure asymmetric quantum mds codes from css construction: A complete characterization. *International Journal of Quantum Information*, *11*(03), 1350027.

Ezerman, M. F., Jitman, S., Ling, S., & Pasechnik, D. V. (2013). Css-like constructions of asymmetric quantum codes. *IEEE transactions on information theory*, *59*(10), 6732–6754.

Ezerman, M. F., Ling, S., & Sole, P. (2011). Additive asymmetric quantum codes. *IEEE transactions on information theory*, *57*(8), 5536–5550.

Fan, J., Li, J., Wang, J., Wei, Z., & Hsieh, M.-H. (2021). Asymmetric quantum concatenated and tensor product codes with large z-distances. *IEEE Transactions on Communications*, *69*(6), 3971–3983.

Fan, J., Li, J., Zhou, Y., Hsieh, M.-H., & Poor, H. V. (2022). Entanglement-assisted concatenated quantum codes. *arXiv preprint arXiv:2202.08084*.

Fan, J.-H., Li, J., Chen, H.-W., & Liu, W.-J. (2021). Degenerate asymmetric quantum concatenated codes for correcting biased quantum errors. *Chinese Physics B*, *30*(12), 120302.

Fedorov, A., Steffen, L., Baur, M., da Silva, M. P., & Wallraff, A. (2012). Implementation of a toffoli gate with superconducting circuits. *Nature*, *481*(7380), 170–172.

Feng, Y.-Y., Zhou, J., Zhang, D.-B., & Shi, J.-J. (2022). Parameterized quantum circuits for learning cooperative quantum teleportation. *Advanced Quantum Technologies*, 2200040.

Feynman, R. P. (1985). Quantum mechanical computers. *Optics news*, *11*(2), 11–20.

Flynn, M. J. (1966). Very high-speed computing systems. *Proceedings of the IEEE*, *54*(12), 1901–1909.

Fuentes, P. (2022). Error correction for reliable quantum computing. *arXiv preprint arXiv:2202.08599*.

Gao, G. (2008). Quantum key distribution by comparing bell states. *Optics communications*, *281*(4), 876–879.

Garipelly, R., Kiran, P. M., & Kumar, A. S. (2013). A review on reversible logic gates and their implementation. *International Journal of Emerging Technology and Advanced Engineering*, *3*(3), 417–423.

Ghosh, D., Agarwal, P., Pandey, P., Behera, B. K., & Panigrahi, P. K. (2018). Automated error correction in ibm quantum computer and explicit generalization. *Quantum Information Processing*, *17*(6), 1–24.

Gisin, N. & Pellaux, J.-P. (1992). Polarization mode dispersion: time versus frequency domains. *Optics communications*, *89*(2-4), 316–323.

Giustina, M., Versteegh, M. A., Wengerowsky, S., Handsteiner, J., Hochrainer, A., Phelan, K., Steinlechner, F., Kofler, J., Larsson, J.-Å., Abellán, C., et al. (2015). Significant-loophole-free test of bell's theorem with entangled photons. *Physical review letters*, *115*(25), 250401.

Glaudell, A. N., Waks, E., & Taylor, J. M. (2016). Serialized quantum error correction protocol for high-bandwidth quantum repeaters. *New Journal of Physics*, *18*(9), 093008.

Gottesman, D. (1997). Stabilizer codes and quantum error correction. California Institute of Technology.

Grassl, M. & Beth, T. (1997). A note on non-additive quantum codes. *arXiv preprint quant-ph/9703016*.

Grassl, M., Huber, F., & Winter, A. (2022). Entropic proofs of singleton bounds for quantum error-correcting codes. *IEEE Transactions on Information Theory*.

Grassl, M. & Rotteler, M. (2008). Non-additive quantum codes from goethals and preparata codes. In *2008 IEEE Information Theory Workshop*, 396–400. IEEE.

Guo, F., Liu, T., Wen, Q., & Zhu, F. (2006). Quantum key distribution based on entanglement swapping between two bell states. *International Journal of Quantum Information*, *4*(05), 769–779.

Hanks, M., Munro, W. J., & Nemoto, K. (2020). Decoding quantum error correction codes with local variation. *IEEE Transactions on Quantum Engineering*, *1*, 1–8.

Harrow, A., Hayden, P., & Leung, D. (2004). Superdense coding of quantum states. *Physical review letters*, *92*(18), 187901.

Hayashi, M. (2006). Quantum information. Springer.

Heranmoy, M., Barik, A. K., Biswas, A., Bhattacharjee, A. K., & Pal, A. (2018). Design of quantum cost, garbage output and delay optimized bcd to excess-3 and 2's complement code converter. *Journal of Circuits, Systems and Computers*, *27*(12), 1850184.

Hogg, T. & Portnov, D. (2000). Quantum optimization. *Information Sciences*, *128*(3-4), 181–197.

Holmes, A., Jokar, M. R., Pasandi, G., Ding, Y., Pedram, M., & Chong, F. T. (2020). Nisq+: Boosting quantum computing power by approximating quantum error correction. In *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)*, 556–569. IEEE.

Honjo, T., Nam, S. W., Takesue, H., Zhang, Q., Kamada, H., Nishida, Y., Tadanaga, O., Asobe, M., Baek, B., Hadfield, R., et al. (2008). Long-distance entanglement-based quantum key distribution over optical fiber. *Optics Express*, *16*(23), 19118–19126.

Hornberger, K. (2009). Introduction to decoherence theory. In *Entanglement and decoherence* 221–276. Springer.

Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. *Reviews of modern physics*, *81*(2), 865.

Horoshko, D., Patera, G., & Kolobov, M. (2019). Quantum teleportation of qudits by means of generalized quasi-bell states of light. *Optics Communications*, *447*, 67–73.

Hu, X.-M., Huang, C.-X., Sheng, Y.-B., Zhou, L., Liu, B.-H., Guo, Y., Zhang, C., Xing, W.-B., Huang, Y.-F., Li, C.-F., & Guo, G.-C. (2021). Long-distance entanglement purification for quantum communication. *Phys. Rev. Lett.*, *126*, 010503.

Huang, C.-X., Hu, X.-M., Liu, B.-H., Zhou, L., Sheng, Y.-B., Li, C.-F., & Guo, G.-C. (2022). Experimental one-step deterministic polarization entanglement purification. *Science Bulletin*, *67*(6), 593–597.

Jackson, T., Grassl, M., & Zeng, B. (2016). Codeword stabilized quantum codes for asymmetric channels. In *2016 IEEE International Symposium on Information Theory (ISIT)*, 2264–2268. IEEE.

Ji, Z., Fan, P., & Zhang, H. (2022). Entanglement swapping for bell states and greenberger–horne–zeilinger states in qubit systems. *Physica A: Statistical Mechanics and its Applications*, *585*, 126400.

Jia, W., Feng, B., Yu, H., & Bian, Y. (2019). Quantum key distribution protocol based on css error correcting codes. In *Proceedings of the ACM Turing Celebration Conference-China*, 1–8.

Jogenfors, J., Elhassan, A. M., Ahrens, J., Bourennane, M., & Larsson, J.-Å. (2015). Hacking the bell test using classical light in energy-time entanglement–based quantum key distribution. *Science Advances*, *1*(11), e1500793.

Josephson, B. D. (1988). Limits to the universality of quantum mechanics. *Foundations of Physics*, *18*(12), 1195–1204.

Khalifa, O. O., Amirah bt Sharif, N., Saeed, R. A., Abdel-Khalek, S., Alharbi, A. N., & Alkathiri, A. A. (2021). Digital system design for quantum error correction codes. *Contrast Media & Molecular Imaging*, *2021*.

Kheirandish, D., Haghparast, M., Reshadi, M., & Hosseinzadeh, M. (2021). Efficient designs of reversible sequential circuits. *The Journal of Supercomputing*, *77*(12), 13828–13862.

Knill, E., Laflamme, R., & Viola, L. (2000). Theory of quantum error correction for general noise. *Physical Review Letters*, *84*(11), 2525.

Kuo, Y.-M., Garcia-Herrero, F., Ruano, O., & Maestro, J. A. (2022). Risc-v galois field isa extension for non-binary error-correction codes and classical and post-quantum cryptography. *IEEE Transactions on Computers*.

La Guardia, G. G. (2013). Asymmetric quantum codes: new codes from old. *Quantum information processing*, *12*(8), 2771–2790.

Landauer, R. (1961). Irreversibility and heat generation in the computing process. *IBM journal of research and development*, *5*(3), 183–191.

Landes, T., Allgaier, M., Merkouche, S., Smith, B. J., Marcus, A. H., & Raymer, M. G. (2021). Experimental feasibility of molecular two-photon absorption with isolated time-frequency-entangled photon pairs. *Physical Review Research*, *3*(3), 033154.

Lang, R. & Shor, P. W. (2007). Nonadditive quantum error correcting codes adapted to the ampltitude damping channel. *arXiv preprint arXiv:0712.2586*.

Leditzky, F., Leung, D., Siddhu, V., Smith, G., & Smolin, J. A. (2022). Generic nonadditivity of quantum capacity in simple channels. *arXiv preprint arXiv:2202.08377*.

Li, J. (2020). Some progress on quantum error correction for discrete and continuous error models. *IEEE Access*, *8*, 46998–47012.

Li, M., Tromp, J., & Vitányi, P. (1998). Reversible simulation of irreversible computation. *Physica D: Nonlinear Phenomena*, *120*(1-2), 168–176.

Li, M.-H., Wu, C., Zhang, Y., Liu, W.-Z., Bai, B., Liu, Y., Zhang, W., Zhao, Q., Li, H., Wang, Z., et al. (2018). Test of local realism into the past without detection and locality loopholes. *Physical review letters*, *121*(8), 080404.

Li, W., Wang, L., & Zhao, S. (2022). Extended single-photon entanglement-based phase-matching quantum key distribution. *Quantum Information Processing*, *21*(4), 1–12.

Liu, B., Liu, X., & Jia, W. (2022). Gllp proof with two-way entanglement purification in quantum key distribution. *The European Physical Journal Plus*, *137*(4), 412.

Liu, W.-Z., Li, M.-H., Ragy, S., Zhao, S.-R., Bai, B., Liu, Y., Brown, P. J., Zhang, J., Colbeck, R., Fan, J., et al. (2021). Device-independent randomness expansion against quantum side information. *Nature Physics*, *17*(4), 448–451.

Liu, X., Liu, J., Xue, R., Wang, H., Li, H., Feng, X., Liu, F., Cui, K., Wang, Z., You, L., et al. (2022). 40-user fully connected entanglement-based quantum key distribution network without trusted node. *PhotoniX*, *3*(1), 1–15.

Liu, X., Yao, X., Xue, R., Wang, H., Li, H., Wang, Z., You, L., Feng, X., Liu, F., Cui, K., et al. (2020). An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution. *APL Photonics*, *5*(7), 076104.

Liu, Y., Yuan, X., Li, M.-H., Zhang, W., Zhao, Q., Zhong, J., Cao, Y., Li, Y.-H., Chen, L.-K., Li, H., et al. (2018). High-speed device-independent quantum random number generation without a detection loophole. *Physical review letters*, *120*(1), 010503.

Lu, L.-C., Ren, B.-C., Wang, X., Zhang, M., & Deng, F.-G. (2020). General quantum entanglement purification protocol using a controlled-phase-flip gate. *Annalen der Physik*, *532*(4), 2000011.

Lu, X. Q., Feng, K. H., & Zhou, P. (2022). Deterministic remote preparation of an arbitrary single-qudit state with high-dimensional spatial-mode entanglement via linear-optical elements. *International Journal of Theoretical Physics*, *61*(2), 1–13.

Luo, C.-C., Zhou, L., Zhong, W., & Sheng, Y.-B. (2021). Multipartite entanglement purification using time-bin entanglement. *Laser Physics Letters*, *18*(6), 065205.

Lv, J., Li, R., & Yao, Y. (2021). Quasi-cyclic constructions of asymmetric quantum error-correcting codes. *Cryptography and Communications*, *13*(5), 661–680.

Ma, F., Gao, J., & Fu, F.-W. (2019). New non-binary quantum codes from constacyclic codes over\begin {document} \mathbb {F} _q [u, v]/\langle u^{2}-1, v^{2}-v, uv-vu\rangle

\

end {document}. *Advances in Mathematics of Communications*, *13*(3), 421.

Maity, H., Biswas, A., Bhattacharjee, A., & Pal, A. (2018). Quantum cost optimized design of 4-bit reversible universal shift register using reduced number of logic gate. *International Journal of Quantum Information*, *16*(02), 1850016.

Maity, H., Biswas, A., Bhattacharjee, A. K., & Pal, A. (2020). The quantum cost optimized design of 2: 4 decoder using the new reversible logic block. *Micro and Nanosystems*, *12*(3), 146–148.

Majumder, A., Singh, P. L., Mishra, N., Mondal, A. J., & Chowdhury, B. (2015). A novel delay & quantum cost efficient reversible realization of 2 i× j random access memory. In *2015 International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI-SATA)*, 1–6. IEEE.

Mamun, M., Al, S., & Menville, D. (2014). Quantum cost optimization for reversible sequential circuit. *arXiv preprint arXiv:1407.7098*.

Martinez, J. E. (2022). Decoherence and quantum error correction for quantum computing and communications. *arXiv preprint arXiv:2202.08600*.

Matsumoto, R. (2020). Improved gilbert-varshamov bound for entanglement-assisted asymmetric quantum error correction by symplectic orthogonality. *arXiv preprint arXiv:2003.00668*.

McClean, J. R., Jiang, Z., Rubin, N. C., Babbush, R., & Neven, H. (2020). Decoding quantum errors with subspace expansions. *Nature communications*, *11*(1), 1–9.

McEwen, M., Kafri, D., Chen, Z., Atalaya, J., Satzinger, K., Quintana, C., Klimov, P. V., Sank, D., Gidney, C., Fowler, A., et al. (2021). Removing leakage-induced correlated errors in superconducting quantum error correction. *Nature communications*, *12*(1), 1–7.

Mohammadi, M., Eshghi, M., Haghparast, M., & Bahrololoom, A. (2008). Design and optimization of reversible bcd adder/subtractor circuit for quantum and nanotechnology based systems. *World Applied Sciences Journal*, *4*(6), 787–792.

Molotkov, S. (2022). ‘pushing’keys through quantum networks and the complexity of search of the true key. *Laser Physics Letters*, *19*(4), 045201.

Montaser, R., Younes, A., & Abdel-Aty, M. (2015). Improving the quantum cost of nct-based reversible circuit. *Quantum Information Processing*, *14*(4), 1249–1263.

Nadlinger, D., Drmota, P., Nichol, B., Araneda, G., Main, D., Srinivas, R., Lucas, D., Ballance, C., Ivanov, K., Tan, E.-Z., et al. (2022). Experimental quantum key distribution certified by bell’s theorem. *Nature*, *607*(7920), 682–686.

Nielsen, M. A. & Caves, C. M. (1997). Reversible quantum operations and their application to teleportation. *Physical Review A*, *55*(4), 2547.

Ofek, N., Petrenko, A., Heeres, R., Reinhold, P., Leghtas, Z., Vlastakis, B., Liu, Y., Frunzio, L., Girvin, S., Jiang, L., et al. (2016). Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, *536*(7617), 441–445.

Ouyang, Y. & Lai, C.-Y. (2022). Linear programming bounds for approximate quantum error correction over arbitrary quantum channels. *IEEE Transactions on Information Theory*.

Paler, A. & Basmadjian, R. (2022). Energy cost of quantum circuit optimisation: Predicting that optimising shor’s algorithm circuit uses 1 gwh. *ACM Transactions on Quantum Computing*, *3*(1), 1–14.

Pan, J.-W., Simon, C., Brukner, Č., & Zeilinger, A. (2001). Entanglement purification for quantum communication. *Nature*, *410*(6832), 1067–1070.

Pan, Y. & Nguyen, T. (2016). Stabilizing quantum states and automatic error correction by dissipation control. *IEEE Transactions on Automatic Control*, *62*(9), 4625–4630.

Pandey, P., Kumari, K., Prathima, A., Mummaneni, K., et al. (2022). Optimized design of alu using reversible gates. In *Proceedings of the International Conference on Computational Intelligence and Sustainable Technologies*, 53–61. Springer.

Pang, S., Xu, H., & Chen, M. (2022). Construction of binary quantum error-correcting codes from orthogonal array. *Entropy*, *24*(7), 1000.

Patel, R. B., Ho, J., Ferreyrol, F., Ralph, T. C., & Pryde, G. J. (2016). A quantum fredkin gate. *Science advances*, *2*(3), e1501531.

Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A., & Kurtsiefer, C. (2009). Daylight operation of a free space, entanglement-based quantum key distribution system. *New Journal of Physics*, *11*(4), 045007.

Pendry, J. B. (1983). Quantum limits to the flow of information and entropy. *Journal of Physics A: Mathematical and General*, *16*(10), 2161.

Peres, A. (1985). Reversible logic and quantum computers. *Physical review A*, *32*(6), 3266.

Qin, L., Li, Y., & Wang, S. (2021). A key distribution protocol based on quantum entanglement swapping for unmanned surface vehicle. In *Journal of Physics: Conference Series*, volume 1976, 012034. IOP Publishing.

Qiskit, Gadi, e. a. (2019). Qiskit: An open-source framework for quantum computing. *Zenodo*.

Qiu, X. & Chen, L. (2022). Quantum cost of dense coding and teleportation. *arXiv preprint arXiv:2202.12544*.

Rahman, M. M., Banerjee, A., Dueck, G. W., & Pathak, A. (2011). Two-qubit quantum gates to reduce the quantum cost of reversible circuit. In *2011 41st IEEE International Symposium on Multiple-Valued Logic*, 86–92. IEEE.

Rains, E. M., Hardin, R. H., Shor, P. W., & Sloane, N. J. A. (1997). A nonadditive quantum code. *Physical Review Letters*, *79*(5), 953–954.

Razeghi, M. (2010). Technology of quantum devices. Springer.

Remón, P., Ferreira, R., Montenegro, J.-M., Suau, R., Pérez-Inestrosa, E., & Pischel, U. (2009). Reversible molecular logic: a photophysical example of a feynman gate. *ChemPhysChem*, *10*(12), 2004–2007.

Ribordy, G., Brendel, J., Gautier, J.-D., Gisin, N., & Zbinden, H. (2000). Long-distance entanglement-based quantum key distribution. *Physical Review A*, *63*(1), 012309.

Riste, D., Poletto, S., Huang, M.-Z., Bruno, A., Vesterinen, V., Saira, O.-P., & DiCarlo, L. (2015). Detecting bit-flip errors in a logical qubit using stabilizer measurements. *Nature communications*, *6*(1), 1–6.

Roffe, J. (2019). Quantum error correction: an introductory guide. *Contemporary Physics*, *60*(3), 226–245.

Roffe, J., Cohen, L. Z., Quintivalle, A. O., Chandra, D., & Campbell, E. T. (2022). Bias-tailored quantum ldpc codes. *arXiv preprint arXiv:2202.01702*.

Roychowdhury, V. P. & Vatan, F. (1998). On the existence of nonadditive quantum codes. In *NASA International Conference on Quantum Computing and Quantum Communications*, 325–336. Springer.

Ryan-Anderson, C., Bohnet, J., Lee, K., Gresh, D., Hankin, A., Gaebler, J., Francois, D., Chernoguzov, A., Lucchetti, D., Brown, N., et al. (2021). Realization of real-time fault-tolerant quantum error correction. *Physical Review X*, *11*(4), 041058.

Şahinkaya, S., Korban, A., & Ustun, D. (2022). Maximal entanglement-assisted quantum error correction codes from the skew group ring $\{\backslash mathbb\{f\}\}\_4\backslash rtimes\_\{\backslash varphi\}gf4\varphi$ g by a heuristic search scheme. *Quantum Information Processing*, *21*(4), 1–19.

Sarvepalli, P. K., Klappenecker, A., & Rötteler, M. (2009). Asymmetric quantum codes: constructions, bounds and performance. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *465*(2105), 1645–1672.

Sasanian, Z., Wille, R., & Miller, D. M. (2012). Realizing reversible circuits using a new class of quantum gates. In *DAC Design Automation Conference 2012*, 36–41. IEEE.

Shalm, L. K., Meyer-Scott, E., Christensen, B. G., Bierhorst, P., Wayne, M. A., Stevens, M. J., Gerrits, T., Glancy, S., Hamel, D. R., Allman, M. S., et al. (2015). Strong loophole-free test of local realism. *Physical review letters*, *115*(25), 250402.

Shalm, L. K., Zhang, Y., Bienfang, J. C., Schlager, C., Stevens, M. J., Mazurek, M. D., Abellán, C., Amaya, W., Mitchell, M. W., Alhejji, M. A., et al. (2021). Device-independent randomness expansion with entangled photons. *Nature Physics*, *17*(4), 452–456.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, *28*(4), 656–715.

Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum key distribution secured optical networks: a survey. *IEEE Open Journal of the Communications Society*.

Sheng, Y.-B. & Zhou, L. (2014). Deterministic polarization entanglement purification using time-bin entanglement. *Laser Physics Letters*, *11*(8), 085203.

Shi, Y., Moe Thar, S., Poh, H. S., Grieve, J. A., Kurtsiefer, C., & Ling, A. (2020). Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber. *Applied Physics Letters*, *117*(12), 124002.

Shnirman, A., Makhlin, Y., & Schön, G. (2002). Noise and decoherence in quantum two-level systems. *Physica Scripta*, *2002*(T102), 147.

Shor, Calderbank, A. R., Rains, Eric M, P., & Sloane, N. J. (1998). Quantum error correction via codes over gf (4). *IEEE Transactions on Information Theory*, *44*(4), 1369–1387.

Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. *Physical review A*, *52*(4), R2493.

Shor, P. W. (1996). Fault-tolerant quantum computation. In *Proceedings of 37th conference on foundations of computer science*, 56–65. IEEE.

Sidana, T. & Kashyap, N. (2022). Entanglement-assisted quantum error-correcting codes over local frobenius rings. *arXiv preprint arXiv:2202.00248*.

Singh Gill, S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., & Buyya, R. (2020). Quantum computing: A taxonomy, systematic review and future directions. *arXiv e-prints*, arXiv–2010.

Slimani, A., Benslama, A., & Misra, N. K. (2022). Optimal designs of reversible/quantum decoder circuit using new quantum gates. *International Journal of Theoretical Physics*, *61*(3), 1–19.

Smolin, J. A., Smith, G., & Wehner, S. (2007). Simple family of nonadditive quantum codes. *Physical review letters*, *99*(13), 130505.

Song, D. (2004). Secure key distribution by swapping quantum entanglement. *Physical Review A*, *69*(3), 034301.

Steane, A. (1996a). Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, *452*(1954), 2551–2577.

Steane, A. M. (1996b). Error correcting codes in quantum theory. *Physical Review Letters*, *77*(5), 793.

Streltsov, A., Kampermann, H., & Bruß, D. (2012). Quantum cost for sending entanglement. *Physical review letters*, *108*(25), 250501.

Sundaresan, N., Yoder, T. J., Kim, Y., Li, M., Chen, E. H., Harper, G., Thorbeck, T., Cross, A. W., Córcoles, A. D., & Takita, M. (2022). Matching and maximum likelihood decoding of a multi-round subsystem quantum error correction experiment. *arXiv preprint arXiv:2203.07205*.

Szyprowski, M. & Kerntopf, P. (2011). An approach to quantum cost optimization in reversible circuits. In *2011 11th IEEE International Conference on Nanotechnology*, 1521–1526. IEEE.

Tornberg, L., Wallquist, M., Johansson, G., Shumeiko, V., & Wendin, G. (2008). Implementation of the three-qubit phase-flip error correction code with superconducting qubits. *Physical Review B*, *77*(21), 214528.

Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., et al. (2007). Entanglement-based quantum communication over 144 km. *Nature physics*, *3*(7), 481–486.

Verma, R. K., Prakash, O., Islam, H., & Singh, A. (2022). New non-binary quantum codes from skew constacyclic and additive skew constacyclic codes. *The European Physical Journal Plus*, *137*(2), 1–13.

Vernam, G. S. (1926). Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, *45*(2), 109–115.

Wagner, T., Kampermann, H., & Bruß, D. (2018). Analysis of quantum error correction with symmetric hypergraph states. *Journal of Physics A: Mathematical and Theoretical*, *51*(12), 125302.

Wagner, T., Kampermann, H., Bruß, D., & Kliesch, M. (2021). Pauli channels can be estimated from syndrome measurements in quantum error correction. *arXiv preprint arXiv:2107.14252*.

Wang, J. & Huberman, B. A. (2022). An overview on deployment strategies for global quantum key distribution networks. *Wireless Communications and Mobile Computing*, *2022*.

Wang, J., Li, R., Lv, J., Guo, G., & Liu, Y. (2019). Entanglement-assisted quantum error correction codes with length $n = \hat{q}2 + 1n = q2 + 1$. *Quantum Information Processing*, *18*(9), 1–21.

Wang, X. & Wilde, M. M. (2020). Cost of quantum entanglement simplified. *Physical Review Letters*, *125*(4), 040502.

Wen-Zhao, L., Zhang, Y.-Z., Zhen, Y.-Z., Li, M.-H., Liu, Y., Fan, J., Xu, F., Zhang, Q., & Pan, J.-W. (2022). Toward a photonic demonstration of device-independent quantum key distribution. *Physical Review Letters*, *129*(5), 050502.

Wilde, M. M., Krovi, H., & Brun, T. A. (2007). Entanglement-assisted quantum error correction with linear optics. *Physical Review A*, *76*(5), 052308.

Wille, R., Saeedi, M., & Drechsler, R. (2010). Synthesis of reversible functions beyond gate count and quantum cost. *arXiv preprint arXiv:1004.4609*.

Wootters, W. K. & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, *299*(5886), 802–803.

Wootton, J. R. & Loss, D. (2018). Repetition code of 15 qubits. *Physical Review A*, *97*(5), 052313.

Xu, J., Chen, X., Zhang, R., & Xiao, H. (2022). Purification in entanglement distribution with deep quantum neural network. *Chinese Physics B*.

Yan, H., Zhong, Y., Chang, H.-S., Bienfait, A., Chou, M.-H., Conner, C. R., Dumur, É., Grebel, J., Povey, R. G., & Cleland, A. N. (2022). Entanglement purification and protection in a superconducting quantum network. *Physical Review Letters*, *128*(8), 080504.

Yan, P.-S., Zhou, L., Zhong, W., & Sheng, Y.-B. (2021). Feasible time-bin entanglement purification based on sum-frequency generation. *Opt. Express*, *29*(2), 571–583.

Yan, P.-S., Zhou, L., Zhong, W., & Sheng, Y.-B. (2022). Measurement-based entanglement purification for entangled coherent states. *Frontiers of Physics*, *17*(2), 1–11.

Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., et al. (2017). Satellite-to-ground entanglement-based quantum key distribution. *Physical review letters*, *119*(20), 200501.

Yin, P.-P., Cao, C., Han, Y.-H., Fan, L., & Zhang, R. (2022). Faithful quantum entanglement purification and concentration using heralded high-fidelity parity-check detectors based on quantum-dot-microcavity systems. *Quantum Information Processing*, *21*(1), 1–19.

Young, N. (1988). An introduction to hilbert space. Cambridge university press.

Yu, S., Chen, Q., Lai, C., & Oh, C. (2008). Nonadditive quantum error-correcting code. *Physical review letters*, *101*(9), 090501.

Zhang, C.-Y. & Zheng, Z.-J. (2021). Entanglement-based quantum key distribution with untrusted third party. *Quantum Information Processing*, *20*(4), 1–20.

Zhang, Y., Shalm, L. K., Bienfang, J. C., Stevens, M. J., Mazurek, M. D., Nam, S. W., Abellán, C., Amaya, W., Mitchell, M. W., Fu, H., et al. (2020). Experimental low-latency device-independent quantum randomness. *Physical review letters*, *124*(1), 010505.

Zhi, Q.-J. & Zheng, Q. (2020). Quantum entanglement purification assisted by classical phase noise. *Modern Physics Letters A*, *35*(32), 2050269.

Zhou, H., Lv, K., Huang, L., & Ma, X. (2022). Quantum network: Security assessment and key management. *IEEE/ACM Transactions on Networking*.

Zhou, L. & Sheng, Y.-B. (2021), High-efficient two-step entanglement purification using hyperentanglement.

Zhou, L., Zhong, W., & Sheng, Y.-B. (2020). Purification of the residual entanglement. *Optics Express*, *28*(2), 2291–2301.

Zulehner, A., Paler, A., & Wille, R. (2018). An efficient methodology for mapping quantum circuits to the ibm qx architectures. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *38*(7), 1226–1236.

Publication Details

Journal Papers

1. **Swathi Mummadi**, and Bhawana Rudra (2022). ”An efficient approach for quantum entanglement purification.” *International Journal of Quantum Information*, Volume: 20, Issue: 04, Pages 2250004. DOI 10.1142/S0219749922500046. **(SCIE & Scopus)**

2. **Swathi Mummadi**, and Bhawana Rudra (2022). ”A Novel Approach for Asymmetric Quantum Error Correction With Syndrome Measurement.” *IEEE Access*, Volume: 10, Pages 44669-44676. DOI 10.1109/ACCESS.2022.3170039. **(SCIE & Scopus)**

3. **Swathi Mummadi**, and Bhawana Rudra (2023). ”Practical Demonstration of Quantum Key Distribution Protocol with Error Correction Mechanism.” *International Journal of Theoretical Physics* Volume: 62, Issue: 04, Pages 86. DOI 10.1007/s10773-023-05324-w **(SCI & Scopus)**

4. **Swathi Mummadi**, and Bhawana Rudra (2022), ”Optimization of Quantum Circuits using Cost Effective Quantum Gates”, *International Journal of Computational Science and Engineering*. (**Revisions Submitted**)

5. **Swathi Mummadi**, and Bhawana Rudra (2022), ”Experimental Analysis of an Asymmetric Quantum Error Correction using Entangled Qubits”, *IEEE Transactions on Information Theory*. (**Under Review**)

6. **Swathi Mummadi**, and Bhawana Rudra (2022), ”Quantum Cost Optimization algorithm for Entanglement based Asymmetric Quantum Error Correction”, *Microsystem Technologies-Springer*. (**Under Review**)

Conference Papers

1. **Swathi Mummadi**, and Bhawana Rudra (2021), ”Implementation of reversible logic gates with quantum gates”, In 11^{th} *Annual Computing and Communication Workshop and Conference (CCWC)*, USA, Pages 1557-1563.
DOI: 10.1109/CCWC51732.2021.9376060 **(Scopus Indexed)**

2. **Swathi Mummadi**, and Bhawana Rudra (2022), ”A Novel Architecture for Binary Code to Gray Code Converter Using Quantum Cellular Automata”, In 26^{th} *annual International Conference on Advanced Computing and Communications (ADCOM)*, Edge Analytics. Springer, Singapore. Pages 43-61.
DOI: 10.1007/978-981-19-0019-8_4 **(Core B & Scopus Indexed)**

3. **Swathi Mummadi**, and Bhawana Rudra (2022), ”Novel Encoding method for Quantum Error Correction”, In 12^{th} *Annual Computing and Communication Workshop and Conference (CCWC)*, USA, Pages 1001-1005.
DOI: 10.1109/CCWC54503.2022.9720880 **(Scopus Indexed)**

4. **Swathi Mummadi**, and Bhawana Rudra (2022), ”Experimental Analysis of a Quantum Encoder on various Quantum Systems”, In 13^{th} *IEEE International Conference on Ubiquitous Computing, Electronics and Mobile Communication (UEMCON)*, USA, Pages 0138-0143.
DOI: 10.1109/UEMCON54665.2022.9965678. **(Scopus Indexed)**

Book Chapters

1. **Swathi Mummadi**, and Bhawana Rudra, ”Fundamentals of Quantum Computation and Basic Quantum Gates”, In *Handbook of Research on Quantum Computing for Smart Environments*, IGI Global, 2023. Pages: 1-24. **(Scopus Indexed)**

Curriculum Vitae

Ms. Mummadi Swathi
Full-Time Research Scholar
Department of Information Technology
National Institute of Technology Karnataka
P.O. Srinivasanagar, Surathkal
Mangalore-575 025

Permanent Address

Mummadi Swathi
H.No. 4-9-31/7
Sanjay Nagar
Adilabad, Telangana-504001
Email: mummadiswathi@gmail.com
Mobile: +918886802800.

Academic Records

1. M.Tech. in Computer Science and Engineering from Marri Laxma Reddy Institute of Technology, JNTU Hyderabad 2014.

2. B.Tech. in Computer Science and Engineering from Maheshwara Engineering College, JNTU Hyderabad 2012.

Research Interests

Quantum Computing and Cryptography
Quantum Key Distribution
Quantum Information
Algorithms
Digital Logic Design

Programming Languages

C, CPP, Qiskit, Q#.