Thesis for the Degree of Doctor of Philosophy

Quantum Synchronization and Consensus for Quantum Networks

Muhammad Asad Ullah

Department of Electronics and Information Convergence Engineering

Graduate School

Kyung Hee University

Seoul, Korea

August, 2022

Quantum Synchronization and Consensus for Quantum Networks

by

Muhammad Asad Ullah

Department of Electronics and Information Convergence Engineering

Graduate School

Kyung Hee University

Seoul, Korea

August, 2022

Quantum Synchronization and Consensus for Quantum Networks

by

Muhammad Asad Ullah

Advised by

Dr. Hyundong Shin

Submitted to the Department of Electronics and Information Convergence Engineering

and the Faculty of the Graduate School of

Kyung Hee University in partial fulfillment

of the requirements for the Degree of

Doctor of Philosophy

Dissertation Committee:

Prof. Yun Hee Kim, Ph.D. .....

Prof. Een-Kee Hong, Ph.D. .....

Prof. Haejoon Jung, Ph.D. .....

Prof. Sunghwan Kim, Ph.D. .....

Prof. Hyundong Shin, Ph.D. .....

Abstract

This dissertation presents quantum synchronization and consensus in quantum networks by using quantum resources like counterfactual communication and entanglement across multiple degrees of freedom (DOF) of a photon. The synchronization between distributed clocks can have unprecedented precision through quantum correlations. However, distributed quantum processors require shared phase reference between distributed nodes. Having a shared phase reference is not always possible in the noisy-intermediate scale quantum (NISQ) era, where quantum decoherence severely limits the performance of quantum devices. Therefore, it is crucial to counter such an absence of share phase reference without compromising the precision. In this dissertation, we first embody the problem of shared phase reference in the context of distributed synchronization and consensus. To account for the absence of the shared phase reference phenomenon in the distributed quantum networks, we first devise a method of synchronization oscillators at distributed nodes through multi-DOF entanglement.

We then extend the problem to time synchronization between two clocks in a distributed network and identify the dynamic Cheshire cat effect as an intriguing concept to achieve time synchronization without requiring shared phase reference. We recognize that this effect allows us to develop a scheme where we can counter any adversary that aims to sabotage the clock synchronization procedure. We show that our system for counterfactual clock synchronization is secure without invoking any security-specific quantum protocols like quantum key distribution (QKD) or quantum secure direct communication etc.

Thereon, we extend the two-party synchronization solution to a multi-node network

consensus without a shared phase reference. The distributed nodes achieve consensus in our system even if certain nodes are malicious. We then investigate the security of this consensus for adversarial attacks by an external sabotaging agent either acting independently or making the network nodes do its bidding.

Then, we analyze the practicality of our dynamic Cheshire cat effect-based setups with NISQ devices and consider how our scheme performs in the NISQ-era quantum network setting. For this purpose, we investigate the impact of noise on a counterfactual entanglement distribution scheme, which is the backbone of most NISQ-era quantum networks.

Finally, we investigate some of the most practical quantum consensus schemes, including ours, for practical blockchain consensus. The blockchain consensus problem is one of the most critical problems in the current era of distributed networks. We compare our counterfactual consensus network's performance with its other quantum and classical peers in terms of security, scalability, and decentralization and show how it becomes a natural fit for intra-enterprise small-scale blockchains.

Keywords: Clock synchronization, quantum entanglement, distributed quantum networks, oscillator frequency synchronization, quantum Cheshire cat effect, quantum Zeno effect, Mach-Zehnder interferometer, interferometric invisibility, noisy quantum channels, quantum noise mitigation, shared phase reference, counterfactual quantum computation, Heisenberg-scaled precision, Byzantine agreement, modular computing units, quantum consensus algorithms, quantum secure protocols, private communication.

Contents

List of Figures

Acknowledgements

I am grateful to my supervisor Professor Hyundong Shin for his expert guidance in making this work possible. His impeccable research excellence made me the researcher I am. I am especially thankful for always backing me up and emotional support during my personal hardships. I would also like to acknowledge Dr. Youngmin Jeong for leading me onto the path of this work, Dr. Junaid ur Rehman for his incredible insights and assistance, and Ahmad Farooq and Fakhar Zaman for the intuitive discussions and research collaborations. I want to extend my appreciation to my lab fellows for making our lab an ideal workplace, for their support, and for the amazing discussions we had.

Above all, I am humbly grateful to Allah Almighty for setting the course of my life that brought me to this stage. To Prophet Muhammad (SAW), whose love brings meaning to my life. To my parents, Ghulam Habib and Nazeer Khatoon, and family for their unwavering love, support, and prayers. My awesome wife, Amna Asad, to whom I am indebted for many things great in my life. Her steadfast companionship has brought incredible joy and strength to me. To my children, Muhammad Yahya Ramzan and Muhammad Musa Ramzan, my two lifelines who bring sheer happiness to my life.

To my friends, Ahmad Farooq, Syed Muhammad Kazim, Waseem Hassan, Syed Muhammad Abuzar Rizvi, Wajahat Ali Khan, Uman Khalid, Usman Akhtar, Aunas Manzoor, and many others who made my stay in Kyung Hee university a joy to remember.

Muhammad Asad Ullah

August, 2022

Abbreviations

LO	Local Oscillator
GHZ	Greenberger–Horne–Zeilinger
DQN	Distributed Quantum Network
LOS	Local Oscillator Syntonization
DOF	Degree of Freedom
THz	Terahertz
QFI	Quantum Fisher Information
MSE	Mean Square Error
CSCS	Counterfactual secure Clock Synchronziation
QCS	Quantum Clock Synchronization
AO	Absorptive Object
QZ	Quantum Zeno
CCR	Conditional Counterfactual Rotation
CQZ	Chained Quantum Zeno
BS	Beamsplitter
SRM	Square root measurement
GUS	Geometrically Uniform Symmetry
nm	Nanometer

MITM	Man-in-the-middle
BA	Byzantine Agreement
QBA	Quantum Byzantine Agreement
QKD	Quantum Key Distribution
CBA	Counterfactual Byzantine Agreement
QAO	Quantum Absorptive Object
CRU	Counterfactual Remote Unitary
QER	Quantum Error Rate
PBFT	Practical Byzantine Fault Tolerance
E91	Ekert-91 QKD Protocol
SRF	Shared phase reference
NISQ	Noisy intermediate-scale quantum
DCC	Direct Counterfactual Communication
PBS	Polarization Beamsplitter
IFM	Interaction-free MEasurement
PR	Polarization Rotator
OC	Optical Circulator
MR	Mirror
SM	Switchable Mirror
EP&D	Local Entanglement preparation and then distribution

Notation and Symbols

We use the following notation and symbols throughout this thesis.

$\mathcal{H}_d$	Hilbert space of dimension d
$\|\cdot\rangle$	A column vector in $\mathcal{H}_d$.
$\langle\cdot\|$	Conjugate transpose of $\|\cdot\rangle$.
ρ	Density operator.
$\mathcal{N}$	Generic quantum noise/channel
σ_i	Pauli qubit operators. σ_i $(i = x, y, z)$ are Pauli X, Y , and Z operators respectively.
$\mathcal{F}$	Quantum Fisher Information
$\boldsymbol{U}$	Quantum operator
$\mathcal{K}$	Quantum superoperator
Π_i	Measurement operator

Chapter 1

Introduction

1.1 Dissertation Motivations and Previous Works

Quantum technologies are going through a second revolution. While the first revolution unraveled the very nature of the physical world, the second revolution aims at harnessing this knowledge to develop new revolutionary technologies. These include unconditionally secure communication, ultra-precise clocks, unprecedented computational power through quantum computing, and the development of new materials and drugs. The development of quantum technologies has been quite rapid, considering that the first quantum computer was made available only in 2016 [1]. Many leading companies globally–including IBM and Google– alongside startups like Oxford Quantum Computing etc., have developed noisy quantum computers made of up to 100 qubits [2]. These companies manufacture quantum computers using qubit modalities ranging from the more conventional superconducting qubits to photonic, tapped ions, neutral cold atoms, and nitrogen-vacancy diamond quantum computing systems [3–6]. Currently, companies and research groups envision quantum networks with nodes that may have different modalities of quantum processors since none of them has shown a decisive advantage. Figure 1.1 provides some

of the historical developments for the quantum networks.

For any distributed computing task such as blockchain consensus, synchronization is key. At a device level, clock synchronization is the backbone of the network.

1.1.1 Clock Synchronization and Network Consensus

Clock synchronization is at the heart of every communication, navigation, and distributed computation system [7]. Recently, the optical atomic clock based on $^{171}Yb^{+}$ ion with a systematic relative uncertainty of 3.2×10^{-18} has been presented, which does not lose or gain a second for billions of years [8]. The recent advancements in optical atomic clocks lead to unprecedented stable time scaling for local computation [7]. Harnessing their true potential for distributed operations requires precise desynchronization detection and resynchronization procedures. For such clocks, desynchronization occurs due to the following three common phenomena: 1) shift in timescale, 2) frequency instability of the local oscillator (LO) and 3) systematic inaccuracy in the frequency of the stable LO [7, 9–16].

The term "clock synchronization" refers to synchronizing the time scales (transitions of a frequency standard) provided by two or more clocks [9, 17–19]. These time scales can differ due to frequency or time discrepancy. The frequency discrepancy, usually called clock desyntonization, causes instability and systematic uncertainty in the clock's frequency standard, which signify the fluctuations and deviation of the local oscillator about the transition frequency of underlying atoms, respectively [20–24]. The time discrepancy, usually called clock desynchronization, yields the disagreement in the time scales regardless of stable and synchronized frequency standards [25–32].

When taken to a network level, clock synchronization algorithms become a subset of the much bigger umbrella of network consensus algorithms. Consensus algorithms constitute an agreement between distributed network nodes on a value or decision. They

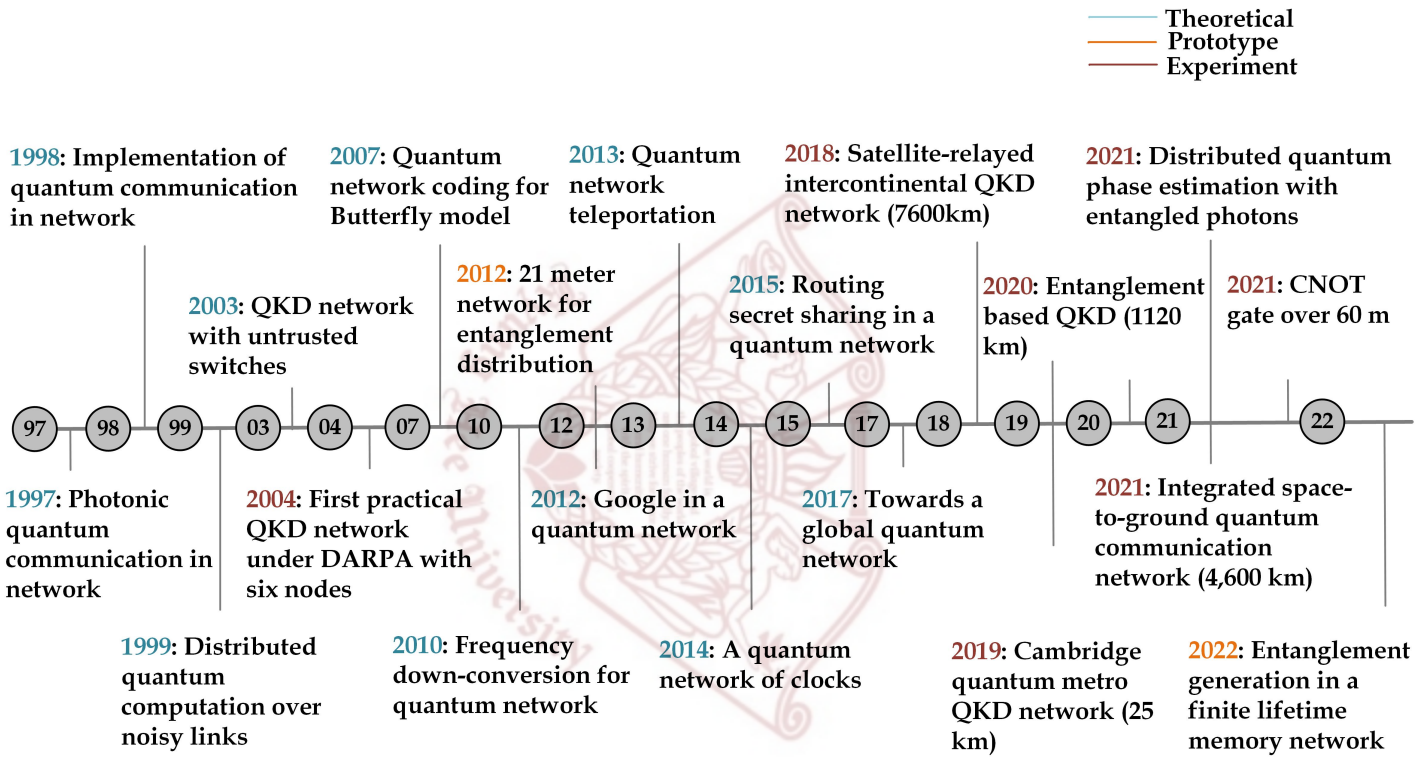


Figure 1.1: Historical developments in the context of quantum networks. Experimental and field demonstrations signify the importance of functional NISQ networks in the near term.

are at the core of cooperative networks and are a factor in determining their performance [33]. Depending on a distributed network's specific nature and resources, its consensus algorithm can be tolerant against crash and/or malicious attack failure. The consensus algorithms that can tolerate malicious attacks are broadly classified under the Byzantine Agreement (BA) umbrella [34].

BA constitutes a consensus between participants in a distributed computation network [34]. BA is based on the "Byzantine three generals problem" in which the commanding general of the Byzantine army wants to broadcast his decision, either attack or defend, to the remaining generals through messengers [35]. Each Lieutenant general decides on the plan of action by considering the messages he receives from the other two generals– however, some of the generals may be traitors. The problem of the Byzantine generals thus constitutes an agreement between the remaining loyal generals. This problem translates to a consensus between non-faulty participants in a distributed network in modern computer systems.

1.1.2 Quantum Solutions for Clock Synchronization and Network Consensus

The use of quantum resources for clock synchronization has its roots in quantum metrology [36]. Quantum algorithms for time synchronization and LO syntonization include the procedures that utilize quantum correlations and the time evolution dynamics of quantum systems for synchronizing the spatially distributed clocks with Heisenberg scaled precision [23, 27–29]. Building on this foundation, [23] proposed a quantum network of clocks that utilizes cascaded GHZ states in centralized network architecture to stabilize the clocks' oscillators. This network achieves unprecedented Heisenberg scaled LO stabilization using nonlocal resources [36].

Quantum correlations allow fast Byzantine agreement, which reduces the complexity

of consensus compared to classical schemes. Quantum Byzantine agreement algorithms enable the communication complexity to be independent of the number of faulty parties. Furthermore, the quantum correlation-based schemes allow detectable BA–a variant of BA which allows abort if loyal nodes cannot agree– even if disloyal parties are more than one-third of the total parties, unlike their classical counterparts [37–40]. Therefore, detectable BA is often referred to as quantum BA (QBA).

1.1.3 Limitations of the Quantum Solutions for Clock Synchronization and Consensus

Absence of Shared Phase Reference

Shared phase reference refers to the existence of common definitions of superposition quantum states, e.g., $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and therefore the definitions of local operators such as Hadamard operation

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

for quantum information processing at distributed nodes (see Figure 1.2). The absence of shared phase reference becomes a problem if the quantum system is prepared at one party and undergoes controlled evolution under nondiagonal operators or noncomputational basis measurement at the other parties. This problem affects almost every task in a distributed quantum network where nodes process non-locally generated qubits, including but not limited to clock synchronization, consensus, quantum key distribution (QKD), blind quantum computation and nonlocal metrology.

Noise in NISQ Devices

To harness the full potential of these quantum technologies, we require complete knowledge of not just the quantum system itself but the actions of their environment decohering

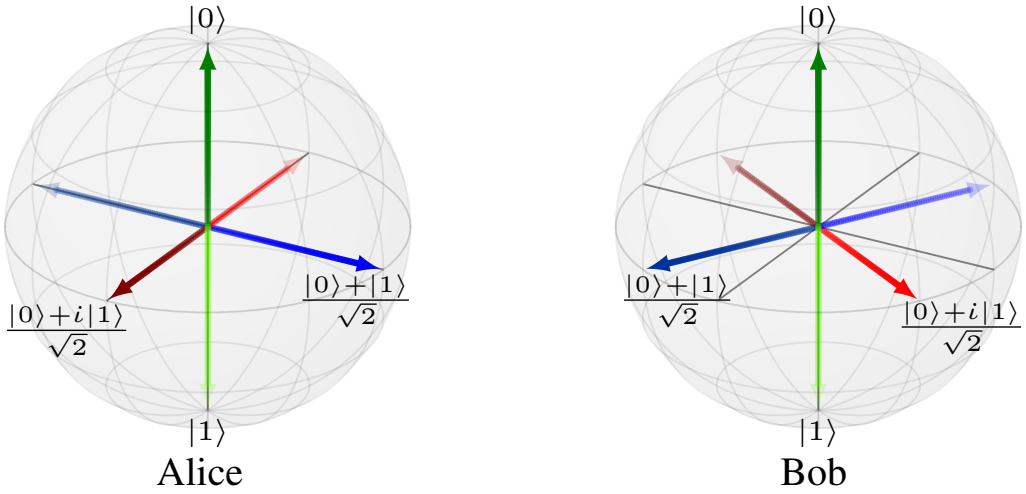


Figure 1.2: Absence of the shared phase reference between Alice and Bob. The states $|0\rangle$ and $|1\rangle$ are equivalent to classical 0 and 1 levels which are the same for the two parties. The other two basis states, which are non-classical, differ for the two parties in this case.

them. In practice, our understanding is still lacking. But that has not stopped the second quantum revolution from developing algorithms and applications for the noisy quantum devices in the current era. Therefore, Preskill has appropriately dubbed the current phase in the development of quantum technologies the "Noisy intermediate-scale quantum (NISQ) era," where factors like environmental decoherence limit the performance of practical quantum algorithms for the clock synchronization and consensus [2].

1.2 Dissertation Contributions and Outline

In this section, we outline the dissertation and describe the main contribution of each chapter with references to the corresponding publications.

Chapter 2

This chapter introduces a distributed quantum network (DQN) for syntonizing (synchronizing the frequency) the oscillators at each node. The proposed scheme does not require a prior quantum handshake or shared phase reference. We counter the need for a shared phase reference by requiring only diagonal quantum unitary operator evolution at distant nodes. Furthermore, the precision achievable in a node's LO syntonization is limited only by its local quantum decoherence.

In our DQN, the branch nodes are noiseless since their local quantum decoherence does not exceed an acceptable threshold. For each new node, we first entangle it with a branch node to integrate it into the DQN. We then perform an overlap measurement at the branch node to estimate noise on the new node. If the noise is within the acceptable threshold, the branch node integrates it as a branch node. Otherwise, it becomes a leaf node in the network. The classification of a node as branch/leaf and the quantitative measurement of local decoherence allows us to optimize our resources for LO resyntonization. Furthermore, we consider two-stage LO resyntonziation. The first stage is for desynchronization detection, which indicates if a node requires resyntonization and provides a rough estimate of this desyntonization. The second stage is LO resyntonization, where we optimally utilize the resources for each node for phase-covariant noise models, including depolarizing and dephasing noise.

Chapter 3

This chapter presents a theoretical proposal to apply the framework of counterfactual quantum communication (which is essentially based on the quantum Cheshire cat effect and the quantum Zeno effect) to synchronize two clocks. The counterfactual communication paradigm allows Bob to deduce Alice's state without exchanging physical particles (photons) between Alice and Bob. Since Alice performs no quantum operation on Bob's

photon, the prior shared phase reference is not required. We design a counterfactual polarization rotator that modifies the photon's polarization. This modification is proportional to the desynchronization between two clocks. We show that the setup provides sub-shot-noise scaling in the precision of the desynchronization estimate. Theoretically, the achievable precision is only a function of the photon duration. For practical single-photon sources producing telecom frequency photon, the photon duration and hence precision can be a tenth of a picosecond. We also establish the security of the clock synchronization scheme by showing that it fulfills both the requirements of protection against channel delay and man-in-the-middle attacks. We use the fact that their counterfactual scheme is probabilistic to our advantage. We use the photons that "accidentally" end up in the channel to detect the presence of an adversary without invoking any quantum key distribution scheme.

Chapter 4

In this chapter, we extend the problem of counterfactual clock synchronization to a network level and consider consensus in the presence of dishonest and faulty parties. Again, our proposed setup is resilient against shared phase reference. For this networked setup, we are especially interested in the security of the consensus scheme. We show that the proposed scheme is secure against all adversarial attack models— including intercept-and-resent, man-in-the-middle, Trojan horse, and entangle-and-measure attack—with the adversary having infinite resources at its disposal. We show that our counterfactual setup provides a very practical model for quantum Byzantine agreement that can be utilized not just for clock synchronization but also for applications like blockchain consensus, secret sharing, anonymous voting, etc.

Chapter 5

This chapter investigates the robustness of our counterfactual setups proposed in Chapters 3 and 4. We consider the effect of noise on the NISQ era quantum devices and networks and how to make our clock synchronization and consensus schemes more practical in NISQ era networks. We propose a modified noise-robust setup for chained quantum Zeno gate to make our counterfactual systems resilient to quantum noise in NISQ devices. We consider the performance of this modified setup for quantum entanglement distribution in the counterfactual Byzantine agreement (Chapter 4). We show that the modification allows better performance of the counterfactual protocols in the NISQ era networks.

Chapter 6

In this chapter, we develop a framework for investigating the practicality of quantum Byzantine agreement algorithms. For this we consider the three performance measures that determine the performance of any consensus algorithm, namely: security, scalability, and decentralization. We utilize the discrete event quantum network simulator NetSquid [41] to design a framework for emulating the quantum Byzantine agreement algorithms under realistic dephasing of optic fiber noise. From chapter 5, we realize that counterfactual BA is robust against natural evolution-based dephasing and the absence of shared phase reference. Our noise analysis further identifies the noise models and their corresponding strengths for comparing the different consensus algorithms. The security analysis allows identifying the algorithms apt at countering an adversary. Finally, the decentralization analysis allows identifying applications where each algorithm can be more useful for decentralized (blockchain consensus) or centralized (clock networks) scenarios. Using the results in chapters 4 and 5, we show that the counterfactual setup outperforms its peers in terms of security and scalability. Hence, making it a possible candidate for the future generation of intra-enterprise consortium blockchain consensus.

Chapter 7

In this chapter we conclude the dissertation by summarizing our main results.

Chapter 2

Quantum Syntonization of Distant Clock Oscillators

Synchronizing distributed frequency standards is a key to distributed computation. Kómár *et al.* proposed a quantum network of clocks, allowing unprecedented precision in stabilizing distributed oscillators [23]. In such a centralized network, the central party estimates the desyntonization via distributed entanglement and stabilizes the oscillators providing frequency standards at each node. In the presence of electromagnetic fields and gravitational effects, a systematic inaccuracy occurs in the affected LO's frequency [7]. In such a scenario, this centralized network will provide inaccurate LO stabilization because the central party stabilizes all LOs to the average deviation during each interrogation cycle. Furthermore, the failure of a single quantum link or a network node in the centralized network will inhibit the clock stabilization for the entire network due to the nature of the multi-partite entangled state. Moreover, the presence of qubit noise (such as local phase-covariant noises [42]) at a single node leads to mixed states, which provide inaccurate and imprecise syntonization of *all* the clock LOs in this network [23, 43]. In this case, the quantum advantage cannot be achieved in precision for any node in the network,

even if it is free of qubit decoherence [23]. The performance may deteriorate to the level where uncorrelated states perform better than multi-partite entangled states because the latter are more vulnerable to quantum noise [44]. Finally, the systematic LO shifts due to external fields may lead to an inaccuracy beyond the dynamic range of stabilization for the higher-order entangled states [7, 43]. Therefore, direct LO stabilization in the centralized network under such systematic shifts leads to inaccurate syntonization.

In this chapter, we focus on countering the systematic frequency inaccuracy of a stable LO with respect to the other clocks' LOs. To this end, we propose a DQN for LO syntonization of distributed clocks, which overcomes the aforementioned shortcomings of the centralized network. By distributing the syntonization control to the branch nodes (Figure 2.1), the LO syntonization in the proposed DQN is robust against quantum losses on a single node. Furthermore, the distributed nature provides a plug-and-syntonize routine for new clocks joining the network.

The remainder of this chapter is organized as follows. In Section 2.1, we provide the context of the desyntonization problem and the utilized resources to tackle this issue. In Section 2.2, we propose the hierarchy of the proposed distributed quantum network for oscillators' syntonization and show the integration process of a new clock in the existing network. Then, we outline our two-step protocol for the clock's local oscillator syntonization (LOS) between two nodes in the distributed network in Section 2.3. Specifically, our discussion up-to and including Theorem 1 outlines the optimal strategy for obtaining the sub-shot noise-limited precision in oscillator syntonization in the presence of local quantum noise. In the remainder of Section 2.3, we compare and discuss the performance of entangled states of the different number of qubits under the given noise conditions. Finally, we conclude our discussion in Section 2.4.

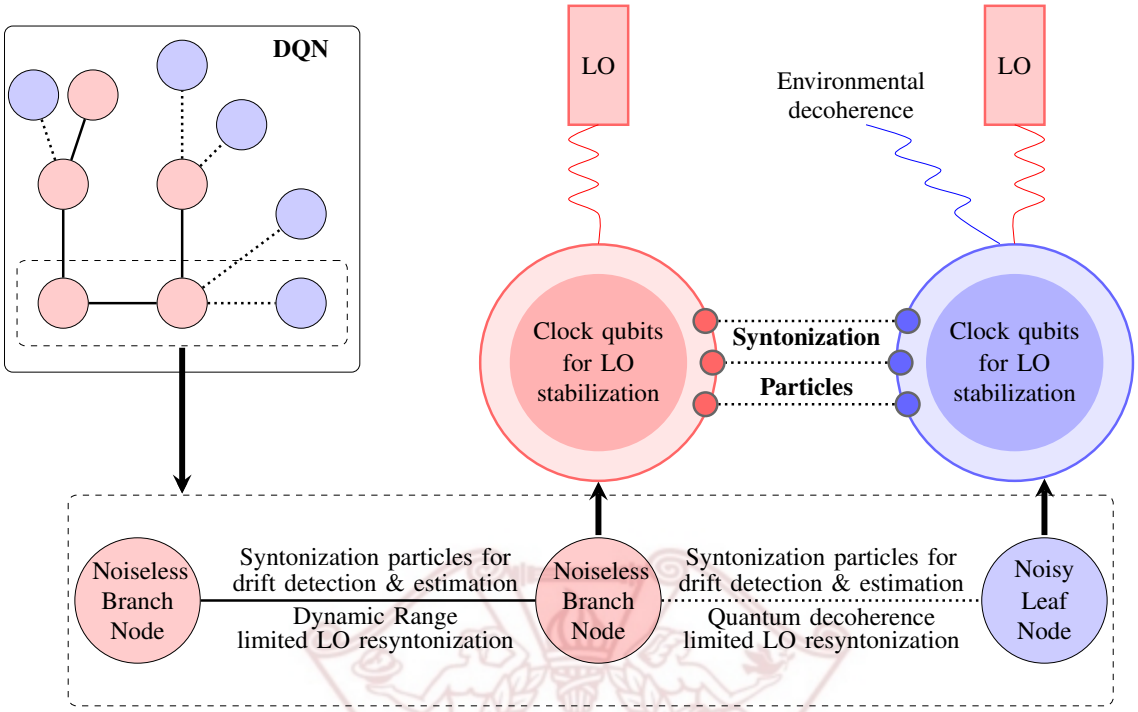


Figure 2.1: DQN for clock LO syntonization. The DQN overcomes: 1) failure of the LOS procedure for the entire network if a single node loses its qubits and 2) degradation in syntonization precision of all the nodes in case of a single node undergoes a phase-covariant noise; both of which may occur when the centralized clock network is subjected to the local qubit noise. Each node in the DQN consists of clock and syntonization particles. The nodes that are unaffected by the local qubit noise form branch nodes in the DQN. Each branch node has the capability of providing LOS for its neighbors. The clock qubits at each node stabilize the LO while syntonization particles are used in the LOS procedure for removing any systematic inaccuracy between the frequencies of the node's LO and the neighboring branch node's LO.

2.1 Clock and Syntonization Resources

Figure 2.1 shows the configuration and functions of two sets of particles; wherein the qubits in clock particles provide the LO stabilization and the syntonization particles are utilized

to detect and remove the systematic inaccuracy in the LO frequency. clock qubits are in the form of cascaded Greenberger–Horne–Zeilinger (GHZ) states which are transitioning at the frequency ω_0 between the high and low energy states of e.g., atoms [7, 23]. LO stabilization is achieved by periodically allowing the clock qubits to evolve freely for a duration $T_c \propto \nu^{-1}$, where ν is the LO frequency, and then performing the interrogation [9].

For an LO of linewidth γ and clock qubits in an N-partite GHZ state, the optimal T_c is given by [45]

$$T_{c,\text{opt}} = \frac{\pi}{\sqrt{2}\gamma\sqrt{\log(\gamma\tau N)}}, \tag{2.1}$$

where τ is the averaging time for the LO stabilization. The maximum LO instability $|\delta|$ which can be mitigated using the local clock qubits is bounded by γ, where $\delta = \nu - \omega_0$ is the shift in the LO frequency. In this range of LO instability, we assume the perfect local LO stabilization using the clock qubits [23].

The syntonization particles in our proposed framework serve two main purposes: i) in the case of new aspirant clocks wishing to join the existing DQN, these syntonization particles are utilized in the characterization of aspirant clocks as leaf or branch nodes. This characterization is performed by estimating the local qubit noise operating on the syntonization particles of aspirant clocks; ii) if the magnitude of the shift is greater than the LO linewidth, the aforementioned local stabilization procedure using the clock qubits fails. This large shift is the manifestation of systematic inaccuracy in the LO frequency which can occur due to a number of environmental factors including gravitational effects and electromagnetic fields causing Zeeman and/or Stark shifts [7]. In our proposed framework of DQN, the shift of this magnitude is detected and removed by cooperatively utilizing the syntonization particles among the neighboring nodes. All physical quantum resources utilized in the syntonization procedure are termed syntonization particles . We utilize two degrees of freedom (DOF) of the syntonization particles, called main and secondary DOFs, with known natural frequencies ω_0 and ω_{0_s} respectively. The purpose of secondary DOF

is to aid the main DOF by estimating the effect of channel delays in LO desyntonization detection and resyntonization.

2.2 Distributed Quantum Network for Oscillators' Syntonization

Figure 2.1 provides the architecture of DQN. The DQN consists of branch nodes and leaf nodes. The qubits in the main DOF of syntonization particles at leaf nodes are affected by the local quantum noise while they are not degraded by this noise at branch nodes. Only the branch nodes in the DQN have the ability to integrate new nodes in the network. The main advantage of the distributed architecture of DQN is the plug-and-syntonize feature for new clocks. In comparison to DQN, a centralized network, the working of the LO syntonization protocol has to be stopped for the entire network before integrating a new clock [23]. This advantage of DQN stems from the capability of branch nodes to independently integrate new clocks to the DQN.

Figure 2.2 shows the procedure for integration of a new clock system in the DQN. The procedure is based on the purity measurement of the evolved singlet states. The purity measurement procedure in both DOFs is the same, therefore, we only describe the procedure for the main DOF here. The integration process is initiated when an aspirant clock (Alice) approaches an existing branch node (Bob) for joining the DQN. Initially, Alice's LO is syntonized with Bob's LO. Bob prepares M singlets $|\Psi^-\rangle = 1/\sqrt{2}\,(|10\rangle - |01\rangle)$ in the main DOF of M pairs of syntonization particles, and sends one particle from each pair to Alice through a noiseless channel. The evolution of local halves of the singlet in the absence of environmental effects is given by $\boldsymbol{U} = e^{itH_0/\hbar}$, where $\hbar$ is the reduced Planck's

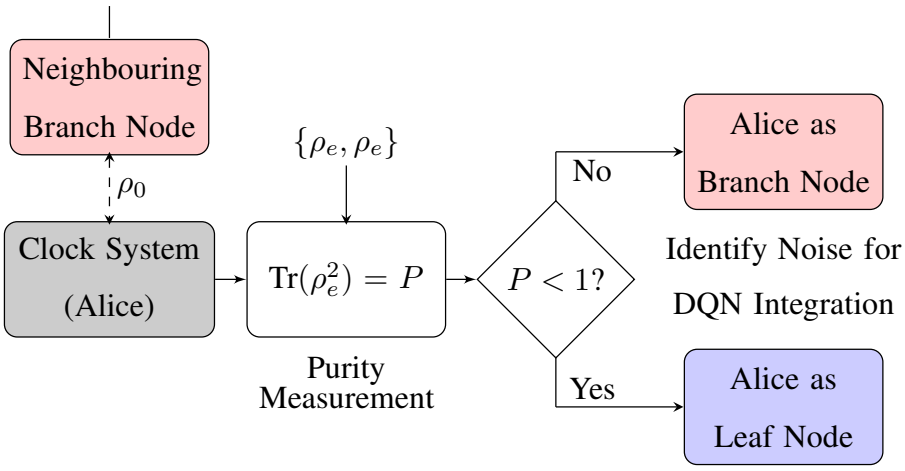


Figure 2.2: The procedure for the integration of a new clock in the DQN through the main DOF of syntonization particles. The neighboring branch node shares entangled qubits in both DOFs of the syntonization particles with the new clock system (Alice) in singlet states. By measuring the purity of these shared singlet states under local dynamics, Alice is designated either as a branch or a leaf node in the DQN. This designation is used during the LOS procedure in the DQN.

constant, t is the total duration of evolution, and

$$\boldsymbol{H}_0 = \frac{\hbar}{2}\begin{bmatrix} \omega_0 & 0 \\ 0 & -\omega_0 \end{bmatrix}, \tag{2.2}$$

is the natural Hamiltonian of qubit evolution. Alice holds the received halves of the singlets at her end for the duration $T_A = \pi/\nu_A$ and allows them to evolve naturally under

$$\boldsymbol{U'} = e^{-iT_A\boldsymbol{H}_0/\hbar} = \begin{bmatrix} -ie^{i\chi/2} & 0 \\ 0 & ie^{-i\chi/2} \end{bmatrix}, \tag{2.3}$$

where $\chi = \delta_A T_A$ with $\delta_A = \nu_A - \omega_0$. The halves that remained at branch node continue to evolve for the same duration. Since for DQN integration, $\nu_{\text{Branch}} = \nu_A$, therefore the evolution of the singlets for the duration T_A is $\boldsymbol{U'}\otimes\boldsymbol{U'}$. After T_A, Alice sends her halves back

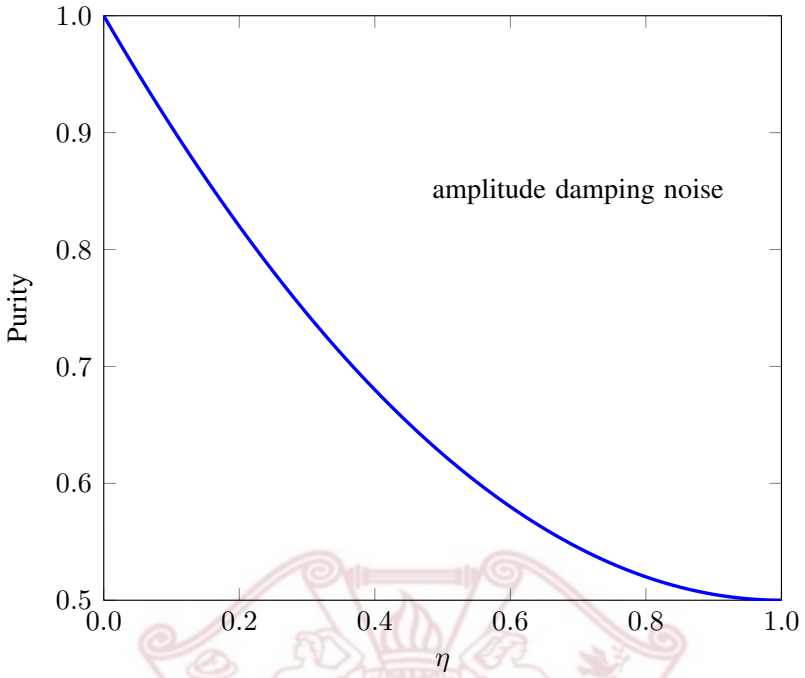


Figure 2.3: Purity of shared Bell state as a function of the noise parameter in amplitude damping noise. The monotonicity of the purity as a function of the noise parameter is used in the LO syntonization procedure.

to Bob. Furthermore, since Alice does not perform any operation on the qubits, therefore no shared phase reference is required between the two clocks [30, 32]. As the natural evolution $\boldsymbol{U}' \otimes \boldsymbol{U}'$ does not change the singlet state, we can identify the presence of noise if the global state is different from the singlet. In order to obtain a quantitative estimate of the qubit noise on Alice's node, the branch node performs the purity measurement on M pairs of the qubits in the main DOF of syntonization particles [46]. M is a function of the required precision ζ in the estimate P. The procedure up-to here is also performed for the secondary DOF for which we estimate the purity estimate P_s. Protocol 1 provides the protocol for DQN integration of a new node.

Alice is admitted in the DQN as a branch node if the qubit evolution was noiseless for

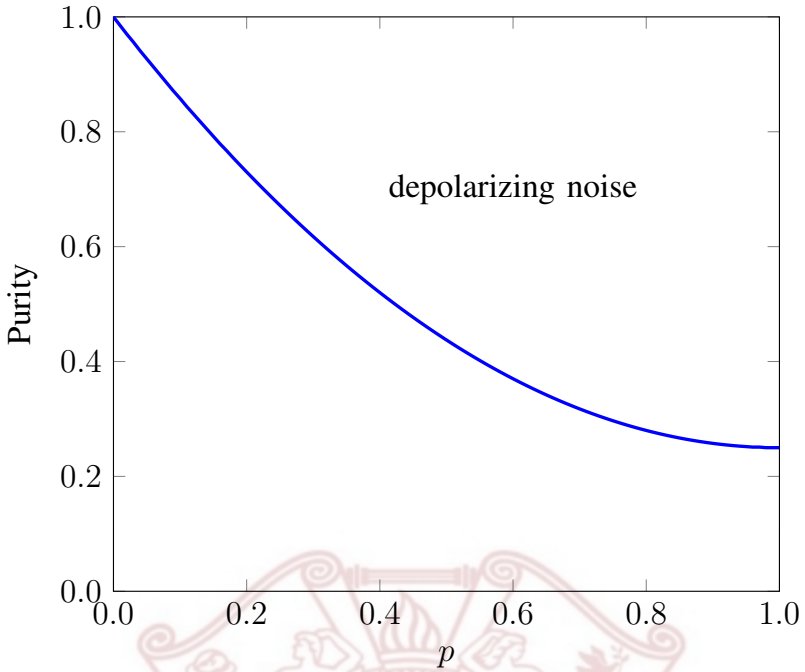


Figure 2.4: Purity of shared Bell state as a function of the noise parameter in depolarizing noise. The monotonicity of the purity as a function of the noise parameter is used in the LO syntonization procedure.

the main DOF i.e., $P = 1$ (Figure 2.2). If the local qubit noise is present at Alice for the main DOF of syntonization particles i.e., $P < 1$, she will be admitted as a leaf node. In the following, we analyze the evolution of the global state and its purity under the local phase-covariant noise.

For both DOFs of the syntonization particles, phase-covariant noise at Alice's node commutes with the global natural unitary of phase evolution at Alice's end. Therefore, without a loss of generality, we can consider that the noise acts initially at $t = t_0$ to lead the pure state to the mixed state $\rho_{t_0}^{\text{noise}}$. Thereafter, the bipartite state $\rho_{t_0}^{\text{noise}}$ evolves only under the unitary dynamics of natural evolution. In the following, we analyze the performance of the proposed scheme in the presence of depolarizing, and amplitude damping noise acting

on either DOFs of Alice's syntonization particles.

- Depolarizing noise

  The depolarizing noise model is the most pessimistic quantum noise as it removes any information carried by the qubit with some probability p [47]. The Kraus operators for depolarizing noise are $\mathcal{K}_0 = \sqrt{1-3p/4}\,\boldsymbol{I}$ and $\mathcal{K}_i = \sqrt{p/4}\,\sigma_i, (i = x, y, z)$, where $\sigma_x,\ \sigma_y, \sigma_z$ are the Pauli matrices. The global evolution of singlet state $\rho_{t_0} = |\Psi^-\rangle\langle\Psi^-|$ with depolarizing noise at Alice's node is

$$\rho_{t_0} \xrightarrow{\mathcal{N}_{\rm de}(\rho)} \rho_{t_0}^{\rm de} = (\mathcal{K}_0 \otimes \boldsymbol{I})\rho_{t_0}(\mathcal{K}_0 \otimes \boldsymbol{I})^\dagger + \sum_{i=x,y,z} (\mathcal{K}_i \otimes \boldsymbol{I})\rho_{t_0}(\mathcal{K}_i \otimes \boldsymbol{I})^\dagger, \tag{2.4}$$

  where

$$\rho_{t_0}^{\rm de} = \begin{bmatrix} p/4 & 0 & 0 & 0 \\ 0 & 1/2 - p/4 & (p-1)/2 & 0 \\ 0 & (p-1)/2 & 1/2 - p/4 & 0 \\ 0 & 0 & 0 & p/4 \end{bmatrix}. \tag{2.5}$$

  The purity of this state is

$$P|_{\rm de} = {\rm Tr}\left((\rho_{t_1}^{\rm de})^2\right) = \frac{3p^2}{4} - \frac{3p}{2} + 1. \tag{2.6}$$

- Amplitude damping noise

  The amplitude damping noise is defined by the Kraus operators, $\mathcal{K}_0 = |0\rangle\langle 0| + \sqrt{1-\eta}\,|1\rangle\langle 1|$ and $\mathcal{K}_1 = \sqrt{\eta}\,|0\rangle\langle 1|$, where $\eta \in [0, 1]$ is the amplitude damping parameter. The singlet state with one half subjected to the noisy map $\mathcal{N}_{\rm ad}(\rho)$ evolves as

$$\rho_{t_0} \xrightarrow{\mathcal{N}_{\rm ad}(\rho)} \rho_{t_0}^{\rm ad} = (\mathcal{K}_0 \otimes \boldsymbol{I})\rho_{t_0}(\mathcal{K}_0 \otimes \boldsymbol{I})^\dagger + (\mathcal{K}_1 \otimes \boldsymbol{I})\rho_{t_0}(\mathcal{K}_1 \otimes \boldsymbol{I})^\dagger, \tag{2.7}$$

which leads the singlet state ρ_{t_0} to

$$\rho_{t_0}^{\text{ad}} = \begin{bmatrix} \eta/2 & 0 & 0 & 0 \\ 0 & 1/2 & -\left(\sqrt{1-\eta}\right)/2 & 0 \\ 0 & -\left(\sqrt{1-\eta}\right)/2 & (1-\eta)/2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{2.8}$$

with purity

$$P|_{\text{ad}} = \text{Tr}\left((\rho_{t_1}^{\text{ad}})^2\right) = 1 + \frac{\eta^2}{2} - \eta. \tag{2.9}$$

The extent to which noise affects the singlet state is dependent on the time duration T_A for which Alice kept the qubits with her since the noise parameters depend on T_A [48]. Afterwards, $\rho_{t_0}^{\text{noise}}$ evolves unitarily to the evolved state $\rho_{t_1}^{\text{noise}}$. For either of the two DOFs of syntonization particles, as long as the noise parameters $(p, \eta) > 0$, we have P (or P_s) < 1. If $P < 1$, Alice is integrated as a leaf node in the DQN. The network configuration is then updated accordingly.

Apart from the characterization of Alice as a branch or leaf node, the purity measurements also provide an estimate on the noise strength of depolarizing and amplitude damping noise in both DOFs of syntonization particles. Figure 2.4 shows the monotonicity of purity P of shared bipartite states against the noise parameter of these models. The same holds for secondary DOF through P_s. An estimate on the purity of the obtained state also provides an estimate on the noise strength of the operating noise models. In the case of amplitude damping noise, $\eta = e^{-\gamma T_A}$, so we know γ, the spontaneous emission rate [49]. Since for $\omega_0 \sim$THz, T_A is of the order of $\sim$femtoseconds; therefore, η will have negligible effect with change in ν_A. Hence, once we know $P(P_s)$, we will use the same η for the LOS procedure. Same is true for depolarizing channel. The purity measurement, therefore, forms the backbone of the LOS procedure for the systematic LO shift estimation since we optimize the LOS procedure by utilizing this information about the noise strength.

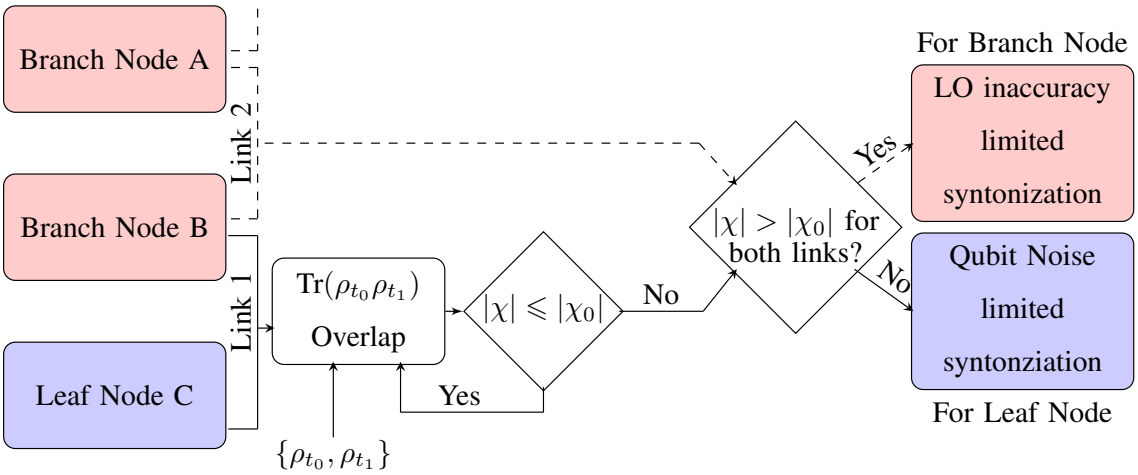


Figure 2.5: LOS procedure in DQN. The first step in the LOS procedure is to probe the DQN to investigate if any node has systematic LO inaccuracy due to external fields (i.e. $|\chi| > |\chi_0|$). This inaccuracy leads to LO shift beyond the stabilizable range of clock qubits. To identify the problematic node, the state with the least sensitivity to LO shift is used. Once the problematic node is identified, the DQN removes the systematic inaccuracy using optimal order GHZ state to bring the LO shift inside the stabilizable range of clock qubits. The precision achieved in the LOS is limited by the amplitude of the LO inaccuracy-based dynamic range for branch nodes and the local qubit noise-based dynamic range for the noisy nodes.

2.3 LOS Procedure for DQN

Now we discuss the procedure of syntonizing the clocks' LOs in the DQN if its LO systematically shifts under the environmental factors such as the gravitational effects and external electromagnetic fields leading to the Zeeman and Stark effect [7, 50]. We counter the LO frequency shift in the following way. If the shift is within the stabilization range of clock qubits, i.e., $|\delta| \leq \gamma$, it is removed by the clock qubits without utilizing the syntonization particles. On the other hand, if the shift is outside the stabilization range of

Protocol 1: Integration of a new clock node (Alice)

(1) **Protocol resources and parameters**

- One main and one secondary degree of freedom (DOF) of each syntonization particle is used.
- ω_0 (ω_{0_s}): The natural frequency of main (secondary) DOF of syntonization particles.
- $\zeta \in \mathbb{R}^{++}$: The precision in purity P of the evolved singlets.
- $M \in \mathbb{N}$,: Singlet states are to be prepared in each DOF as a function of ζ.
- Initially syntonized LO at Alice for DQN integration.

(2) **The Protocol** For both DOFs:

- The M singlets are prepared in both DOFs at the neighboring branch node (Bob).
- Bob sends one particle in each singlet to Alice through a noiseless quantum channel.
- Alice holds the particles for the duration $T_A = \pi/\nu_A = \pi/\nu_{\text{Branch}}$ during which the qubits in each DOF are subject to local quantum noise at Alice.
- Alice sends the particles back to Bob.
- Bob performs purity measurement on each of the M evolved singlet states in both the main and secondary DOFs and stores the result at P and P_s.
- If $P = 1$ in the main DOF, Alice is integrated as a leaf node otherwise it is a branch node.

clock qubits, i.e., $|\delta| > \gamma$, we employ the main DOF of the syntonization particles to first perform the detection of this systematic inaccuracy and then precisely estimate this shift for its mitigation (Figure 2.5). By detecting this inaccuracy before its estimation, we are able to identify the problematic node and hence target all our syntonization resources to the problematic node. The purpose of secondary DOF in both the desyntonization detection and LO resyntonization is to counter the channel delays as explained in the Protocol 2 and Protocol 3. In the subsections 2.3.1 and 2.3.2, we will only discuss the role of the main DOF in LO desyntonization detection and resyntonization.

2.3.1 Desyntonization Detection

The desyntonization detection utilizes the information of Alice being a branch or leaf node to optimize the use of quantum resources under phase covariant noise for quickly detecting the drift [51]. If Alice is a branch node, then Bob prepares single-qubit states $|\phi^+\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle)$ and sends them to Alice. On the other hand, if Alice is a leaf node, Bob prepares Bell states $|\Phi^+\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ and sends one particle of each to Alice. The advantage of using the Bell state for the latter is based on the monotonicity of purity via Figure 2.4.

The evolution of the states in both the cases for the duration of transmission is adjusted by introducing transmission delays such that the introduced relative phase due to channel time delays is an integer multiple of 2π [26, 52]. The purpose of secondary DOF is to counter any nonuniform channel time delay induced phase mod 2π as explained in the protocol 2. Each of the states, $|\phi^+\rangle$ & $|\Phi^+\rangle$, can detect the highest LO shift amplitude albeit with a much lesser precision compared to the higher order entangled quantum systems [43,45]. This is due to the fact that these states are least sensitive to LO frequency inaccuracy [43]. We first consider the desyntonization detection for branch nodes before extending the procedure to the leaf nodes. The protocol for desyntonization detection has

Protocol 2: Desyntonization Detection of Alice's LO

(1) **Protocol resources and parameters**

- One main and one secondary degree of freedom (DOF) of each syntonization particle is used.
- ω_0 (ω_{0_s}): The natural frequency of main (secondary) DOF of syntonization particles.
- $|\chi_0| \in \mathbb{R}^{++}$: The threshold above which drift is to be detected.
- $P(P_s) \in [0, 1]$: The purity of measured singlets in main (secondary) DOF of syntonization particles monotonic with the noise parameters $\eta(p)$ for amplitude damping (depolarizing) noise during DQN integration.
- $\zeta \in \mathbb{R}^{++}$: The precision of the measured purity.
- For the main DOF, $N_{\min} \in \mathbb{N}$,: states are to prepared as a function of $|\chi_0|$ and ζ via eq. (13).
- For the secondary DOF, $N_{\min} \in \mathbb{N}$,: qubits are entangled into copies of $\left(n_{\text{opt}_s}\right)$-partite GHZ states through Theorem 1, Figures 2.10, 2.13, and 2.14 without employing any ancilla.

(2) **The Protocol**

- At the neighboring branch node (Bob),

  – if Alice is a branch node: $N_{\min}$ qubits in $|\phi^+\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle)$ are prepared.

  – else, $N_{\min}$ Bell states in $|\Phi^+\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ are prepared.

been provided as Protocol 2.

Protocol 2: Contd.

(2) Contd.

- Bob sends $N_{\min}$ particles to the branch node Alice through the noiseless quantum channel

  – in the main DOF of these particles, the qubits are in $|\phi^+\rangle$ if Alice is a branch node or halves of $|\Phi^+\rangle$ states if Alice is a leaf node.

  – in the secondary DOF of the particles, n_{opt_s}-partite GHZ states.

- In the main DOF, if Alice is a leaf node, Bob allows evolution of its halves of the $|\Phi^+\rangle$ states for the duration $T_{\text{Branch}} = \pi/\nu_{\text{Branch}}$.

- Alice holds the particles for the duration $T_A = \pi/\nu_A$ during which

  – the qubits in the main DOF are subject to local quantum noise and natural evolution through Hamiltonian in eq. (2). Meanwhile, qubits (ancilla) at Bob are undergoing natural evolution.

  – the qubits in secondary DOF evolve only under the local noise map as Alice stops the evolution for the duration it holds the particles.

- Alice sends the particles back to Bob.

- After receiving the particles,

  – for the main DOF, Bob performs overlap measurement on each of the $N_{\min}$ evolved qubits (or Bell states).

  – for the secondary DOF, Bob performs Ramsey measurement on the n_{opt_s}-partite GHZ states to estimate the channel correction phase mod 2π.

- The result O of the overlap measurement in the main DOF is corrected through phase estimation in the secondary DOF. If the corrected overlap is $O < 1$, LO resyntonization protocol is evoked.

Alice as the Problematic Branch Node

In this event of systematic inaccuracy in the LO frequency, the Alice's LO gets a frequency lag/lead $|\delta_A| = |\nu_A - \nu_{\text{Branch}}| = |\nu_A - \omega_0| > \gamma$ with respect to the neighbouring branch

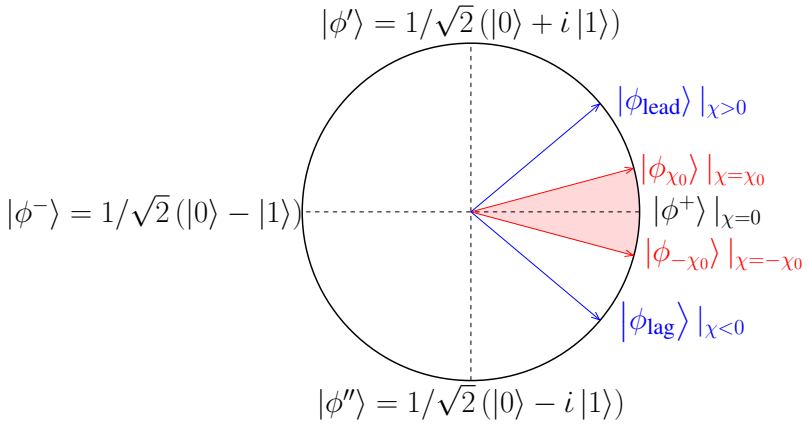


Figure 2.6: Effect of LO frequency shift at the clock's LO. $|\phi^+\rangle$ state evolution in noiseless case ($P = 1$) under the frequency drift unitary U'. The lead/lag caused by the frequency shift evolves the $|\phi^+\rangle$ state to either $|\phi_{\text{lead}}\rangle$ or $|\phi_{\text{lag}}\rangle$. The shaded region corresponds to to the LO fluctuations which are stabilized by the local clock qubits ($|\chi| \leq |\chi_0|$).

node's LO. Alice keeps the qubits for $T_A = \pi/\nu_A$. Therefore, the $|\phi^+\rangle$ state at t_0 evolves locally till t_1 to the state

$$|\phi^+_{t_1}\rangle = \boldsymbol{U'}\,|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{e}^{-i\chi}\,|1\rangle). \tag{2.10}$$

The lag/lead phase χ captures the systematic inaccuracy in Alice's LO and is lower bounded by the upper limit $|\chi_0|$ on the LO stabilization range using clock qubits (Figure 2.7).

The overlap between the two states ρ_{t_1} and ρ_{t_0} can be related to the purity P and the distance between the two states by [51]

$$\begin{aligned}\mathrm{Tr}(\rho_{t_1}\rho_{t_0}) &= \frac{1}{2}\left(P_{\rho_{t_0}} + P_{\rho_{t_1}}\right) - \frac{1}{2}\mathrm{Tr}\left((\rho_{t_0} - \rho_{t_1})^\dagger(\rho_{t_0} - \rho_{t_1})\right) \\ &= 1 - \frac{1}{2}D,\end{aligned} \tag{2.11}$$

where,

$$D = \mathrm{Tr}\left((\rho_{t_1} - \rho_{t_0})^\dagger(\rho_{t_1} - \rho_{t_0})\right) = 1 - \cos(\chi). \tag{2.12}$$

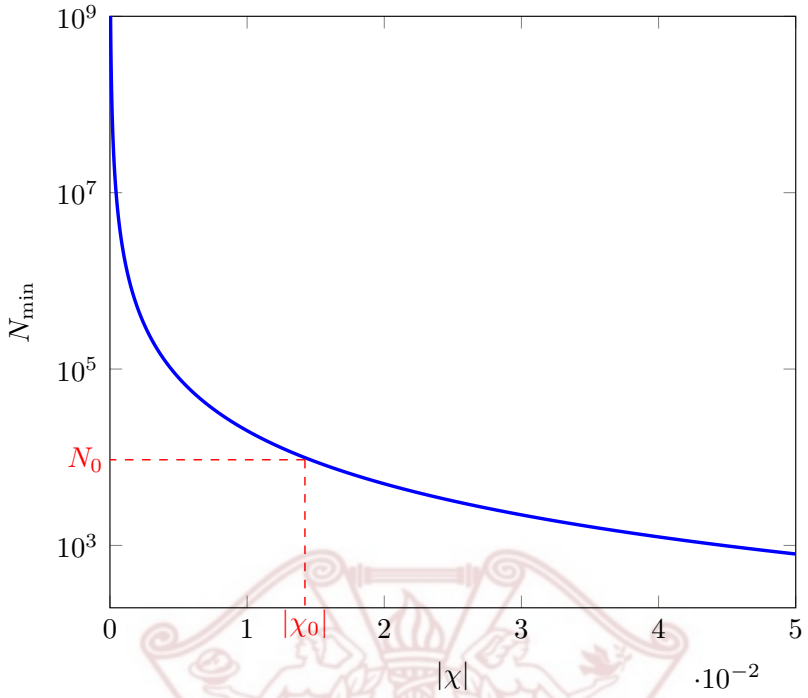


Figure 2.7: Minimum copies $N_{\min}$ of the $|\phi^+\rangle$ state for detecting $|\chi|$ in noiseless case. Given N_0 copies of the state, the synchronization protocol for systematic inaccuracy is invoked at $|\chi| > |\chi_0|$. For shift inside this shaded region, evolved state (of qubits in main DOF of the syntonization particles) for the desyntonization detection procedure is indistinguishable from $|\phi^+\rangle$ using $N_{\min} = N_0$ copies. Therefore the LOS for systematic inaccuracy is not employed in this region.

The minimum number of copies of evolved Bell states required for detecting the systematic shift χ are [51]

$$N_{\min} = \left[\frac{1}{3D}\left(\sqrt{(1+P-\frac{D}{2})(1-P+\frac{D}{2})}+\sqrt{(1+P-2D)(1-P+2D)}\right)\right]^2. \quad (2.13)$$

For $P = 1$, the equation reduces to

$$N_{\min} = \left[\frac{1}{3D}\left(\sqrt{D\left(1-\frac{D}{4}\right)} + \sqrt{4D(1-D)}\right)\right]^2. \tag{2.14}$$

From Figure 5b, given at least N_0 copies, we can successfully detect a shift of $|\chi| > |\chi_0|$ in the state ρ_{t_1} using the state overlap measurement. For a larger range of LO stabilization $|\chi_0|$ of clock qubits, the overlap measurement $\mathrm{Tr}(\rho_{t_0}\rho_{t_1})$ will require lower number of copies of the Bell state for systematic inaccuracy detection.

Alice as the Problematic Leaf Node

If Alice is a leaf node, we utilize shared Bell state $|\Phi^+\rangle$ for desyntonization detection. One half of the Bell states that goes to Alice evolves under $\boldsymbol{U'}$. Meanwhile, the qubit at the Bob is allowed to evolve for $T = \pi/\nu_{\text{Branch}} = \pi/\omega_0$. Hence, the local unitary of evolution at the branch node is

$$\boldsymbol{U}_{\text{Branch}} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.15}$$

Therefore, at the leaf node, in the presence of phase-covariant noise e.g., depolarizing noise, a frequency shift for the duration $t_1 - t_0$ leads the mixed state $\rho_{t_0}^{\text{de}}$ to the state $\rho_{t_1}^{\text{de}}$ under the unitary transformation $\boldsymbol{U'} \otimes \boldsymbol{U}_{\text{Branch}}$. The overlap is

$$\mathrm{Tr}\left(\rho_{t_0}^{\text{de}}\rho_{t_1}^{\text{de}}\right) = P - \frac{D}{2}. \tag{2.16}$$

where for depolarizing noise,

$$D|_{\text{de}} = \mathrm{Tr}\left(\left(\rho_{t_0}^{\text{de}} - \rho_{t_1}^{\text{de}}\right)^\dagger\left(\rho_{t_0}^{\text{de}} - \rho_{t_1}^{\text{de}}\right)\right) = 1 - 2p + p^2 + \left(2p - 1 - p^2\right)\cos(\chi), \tag{2.17}$$

and for the amplitude damping noise,

$$D|_{\text{ad}} = \mathrm{Tr}\left((\rho_{t_0}^{\text{ad}} - \rho_{t_1}^{\text{ad}})^\dagger(\rho_{t_0}^{\text{ad}} - \rho_{t_1}^{\text{ad}})\right) = 1 - \eta - (1-\eta)\cos(\chi). \tag{2.18}$$

The minimum number of copies of the Bell state required for shift detection under depolarizing noise is [51] obtained through (2.13).

Figure 2.9 shows $N_{\min}$ as a function of $|\chi|$ for the depolarizing and amplitude damping noise. As the noise parameter increases, the required number of copies of Bell state to detect the same shift $|\chi_0|$ increases.

In the DQN, to identify the problematic node/nodes, the procedure of shift detection is simultaneously performed for all nodes. From Fig 2.5, branch node B checks if it is syntonized to node A and node C. If it is desyntonized with both, it is the problematic node. Otherwise, if it is syntonized with node A but not node C, then C is the problematic node.

2.3.2 LO Resyntonization

Once the systematic inaccuracy is detected, we estimate the magnitude of LO shift introduced by this systematic inaccuracy. The protocol for LO resyntonization has been summarized as Protocol 3. Use of n-partite GHZ in shift estimation allows the used state to pick up a phase of $n\chi$. A phase-slip error occurs if the introduced relative phase falls outside the interval $(-\pi, \pi)$. These phase-slip errors must be avoided by utilizing n-partite GHZ states such that the magnitude of $n\chi$ is within the interval of no phase-slip errors [43]. Therefore, increasing n will decrease the value of χ causing a phase-slip error. On the other hand, the relative phase due to minimum LO shift is $n|\chi_0|$ which increases with n. Consequently, the range of estimatable LO shift decreases with an increase in the number of qubits n in the GHZ state. The dynamic range of a state for estimating the shift is the ratio between the maximum and the minimum estimatable LO desyntonization using the state [43]. The desyntonization detection by shared Bell states provides an imprecise but maximum dynamic range estimate of the systematic shift. The dynamic range decreases with an increase in the number of qubits n in the n-partite GHZ states.

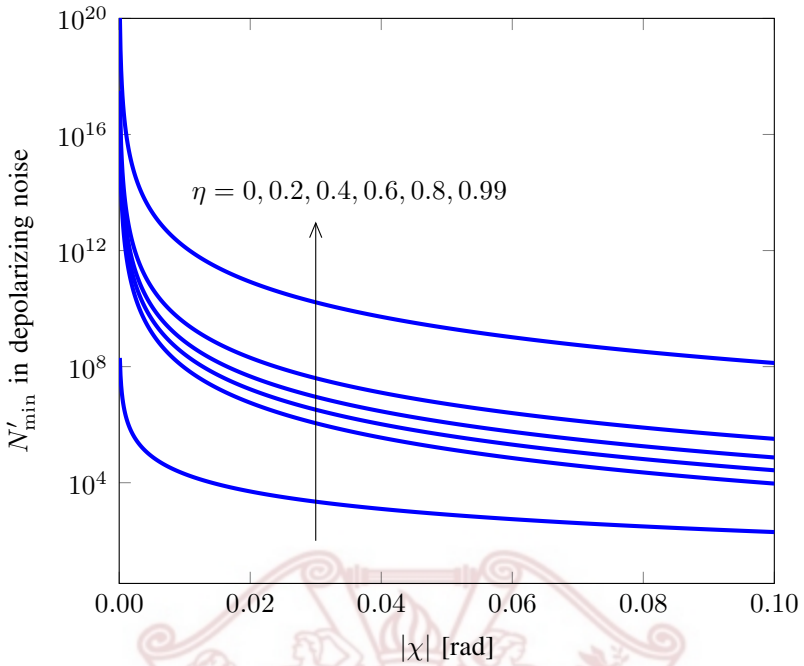


Figure 2.8: Minimum number of copies $N'_{\min}$ of Bell state as a function of shift $|\chi|$ in the presence of amplitude damping noise for shift detection. The upward direction of arrow shows increasing value of noise parameters. As the noise parameters increase, the required number of copies $N_{\min}$ increase. For $\eta \to 1$ and $p \to 1$, $N'_{\min} \to \infty$.

Apart from the dynamic range, the other significant factor in choosing the optimal state for shift estimation is the quantum Fisher information(QFI). For n-partite GHZ states ρ_{GHZ} evolving under shift encoding dynamics, the QFI lower bounds the mean square error (MSE) in the unbiased parameter estimation as [36]

$$\text{MSE}(\hat{\chi_n}) \geq \frac{1}{r\mathcal{F}}, \tag{2.19}$$

where $\mathcal{F}$ is the QFI of ρ_{GHZ} and r is the number of copies utilized in the estimation. The

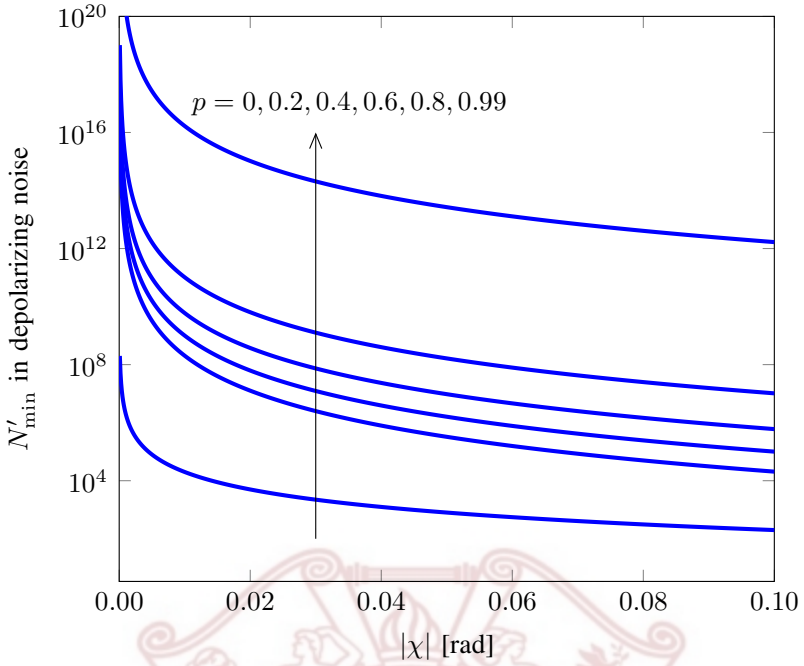


Figure 2.9: Minimum number of copies $N'_{\min}$ of Bell state as a function of shift $|\chi|$ in the presence of depolarizing noise for shift detection. The upward direction of arrow shows increasing value of noise parameters. As the noise parameters increase, the required number of copies $N_{\min}$ increase. For $\eta \to 1$ and $p \to 1$, $N'_{\min} \to \infty$.

QFI is given by [53]

$$\mathcal{F} = \sum_{j=1}^{d} 4\lambda_j \langle \Delta^2 \boldsymbol{H} \rangle_j - \sum_{j \neq k} \frac{8\lambda_j \lambda_k}{\lambda_j + \lambda_k} |\langle \psi_j | \boldsymbol{H} | \psi_k \rangle|^2, \tag{2.20}$$

where $\boldsymbol{H}$ is the generator of the parameter encoding dynamics, and $\langle \Delta^2 \boldsymbol{H} \rangle_j = \langle \psi_j | \boldsymbol{H}^2 | \psi_j \rangle - (\langle \psi_j | \boldsymbol{H} | \psi_j \rangle)^2$ is the variance of $\boldsymbol{H}$ for $|\psi_j\rangle(\lambda_j)$ which are the eigenstates (eigenvalues) of the ρ_{GHZ} while d is the dimensionality of the ρ_{GHZ}. Due to the commutation between phase-covariant noise map and $\boldsymbol{U}'$, we consider that the pure GHZ states at the leaf nodes are first subjected to local noise and the resulting states are used as the probe states at $t = 0$.

Protocol 3: Alice's LO Resyntonization

(1) **Protocol resources and parameters**

- One main and one secondary degree of freedom (DOF) of each syntonization particle is used.
- ω_0 (ω_{0_s}): The natural frequency of main (secondary) DOF of syntonization particles.
- The imprecise $\delta_A \in \mathbb{R}$ achieved through desyntonization detection stage.
- $P(P_s) \in [0, 1]$: The purity of measured singlets in main (secondary) DOF of syntonization particles monotonic with the noise parameters $\eta(p)$ for amplitude damping (depolarizing) noise during DQN integration.
- $\zeta \in \mathbb{R}^{++}$: The precision of the measured purity.
- For the main DOF, $n \in \mathbb{N}$:, qubits are divided into r copies of (n_{opt} + ancilla)-partite GHZ states by considering Theorem 1, Figures 2.10, 2.13, and 2.14.
- For the secondary DOF, The n_{opt}:, qubits are entangled into r' copies of $\left[n_{\text{opt}_s} (\leq n_{\text{opt}})\right]$-partite GHZ states of particles following the same rule as main DOF i.e., through Theorem 1, Figures 2.10, 2.13, and 2.14 without employing any ancilla.

(2) **The Protocol**

- Bob sends n_{opt} particles of the GHZ states of the particles to the Alice.
- Alice holds the particles for the duration $T_A = \pi/\nu_A$ during which

  – the qubits in the main DOF are subject to local quantum noise and natural evolution. Meanwhile, qubits (ancilla) at Bob are undergoing natural evolution.

  – the qubits in secondary DOF evolve only under the local noise map.

Protocol 3: Contd.

(2) Contd.

- Alice sends the n_{opt} particles back to Bob.
- Bob performs Ramsey measurement on each of the evolved entangled qubits to estimate the LO drift δ_A in the main DOF and the correction due to channel in the secondary DOF.
- Bob communicates the corrected δ_A to Alice so that Alice may resyntonize its LO with the network LOs.

In the following, we show how QFI, dynamic range, and the local qubit noise determine the optimal state in shift estimation.

Branch Node

Once the desyntonization has been detected at a branch node (Alice), one of the neighboring branch nodes prepares n-partite GHZ states ρ_{GHZ} and sends them to Alice. Alice keeps the received qubits for the duration π/ν_A and sends them back to the accurate branch node for measurement and post-processing. Each qubit at the problematic node undergoes shift encoding dynamics which depends on the magnitude of LO systematic inaccuracy.

The generator $\boldsymbol{H}$ of shift encoding unitary is [54]

$$\boldsymbol{H} = i\left(\frac{\partial}{\partial\chi}\boldsymbol{U}'^{\otimes n}\right)\left(\boldsymbol{U}'^{\otimes n}\right)^{\dagger}. \tag{2.21}$$

For the noiseless case, the QFI in (2.20) reduces to [36]

$$\mathcal{F} = 4\langle\Delta^2\boldsymbol{H}\rangle = n^2. \tag{2.22}$$

That is, the available Fisher information scales quadratically with the number of particles undergoing shift encoding dynamics and providing Heisenberg $(1/n^2)$ scaling in the mean square error.

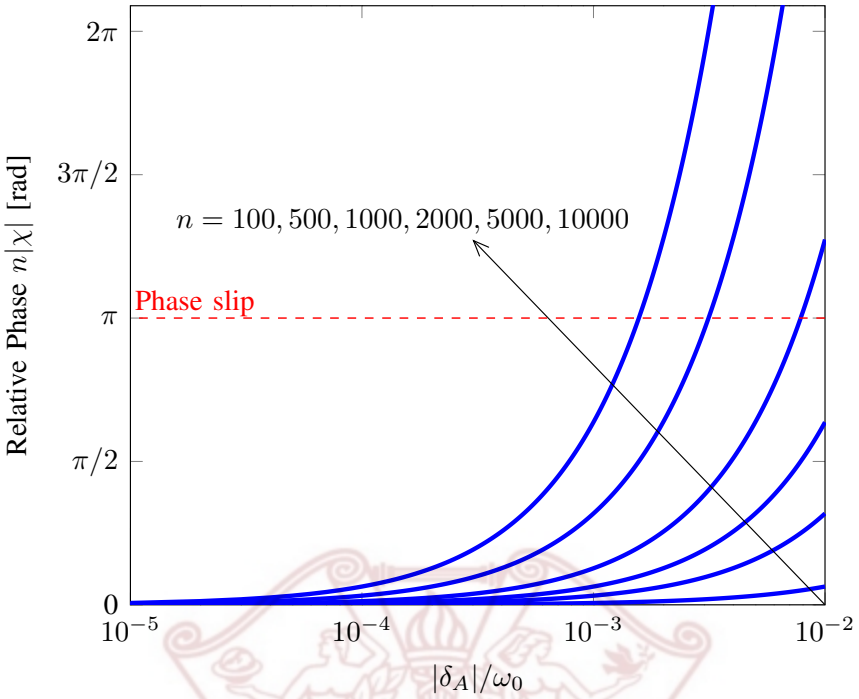


Figure 2.10: Identification of n_{opt} for $\omega_0 = 100$ THz.

If the rough estimate of the LO drift obtained in the detection step indicates that utilizing all n available qubits in main DOF of the syntonization particles in a GHZ form will lead to a phase slip, we make r groups each containing $n_{\text{opt}} = \lfloor n/r \rfloor$ qubits. From Figure 2.10, the drift estimation is now performed by r copies of n_{opt}-partite GHZ states. The scaling in the mean square error in this case is of order r/n^2; thus providing a trade-off between the dynamic range and the optimal scaling in the mean square error.

Leaf Node

The precision in phase estimation increases with the number of qubits n_{opt} in GHZ states. However, the GHZ states become more sensitive to noise at the same time. Hence the accuracy in estimated shift χ decreases with an increase in the qubit noise strength. Fur-

thermore, ancilla qubits provide an advantage in the noise-limited metrology by increasing the achievable QFI [42]. Therefore, we consider $(i+1)$-partite GHZ states, denoted by ρ'_{GHZ}, for the estimation of LO shift where i qubits are sent to Alice and the remaining qubit acts as an ancilla. The following theorem provides the trade-off between the error probability beyond a preselected threshold and the precision of noise-limited LOS for leaf nodes.

Theorem 1. *For a minimum variance unbiased estimate $\hat{\chi}$ of parameter χ, and for any $\epsilon > 0$*

$$\mathbb{P}\{|\hat{\chi} - \chi| \geq \epsilon\} \leq \frac{1}{\mathcal{F} r \epsilon^2}, \tag{2.23}$$

where $\mathbb{P}\{A\}$ is the probability of event A.

Proof. From the Chebyshev's inequality [55]

$$\mathbb{P}\{|\hat{\chi} - \mu(\hat{\chi})| \geq \epsilon\} \leq \frac{\mathrm{Var}(\hat{\chi})}{\epsilon^2}, \tag{2.24}$$

where $\mu(X)$, and $\mathrm{Var}(\hat{X})$ are the mean and variance of a random variable X, respectively.

For an unbiased estimator, $\mu(\hat{\chi}) = \chi$ and MSE $(\hat{\chi}) = \mathrm{Var}(\hat{\chi})$. Therefore

$$\mathbb{P}\{|\hat{\chi} - \chi| \geq \epsilon\} \leq \frac{\mathrm{MSE}(\hat{\chi})}{\epsilon^2}. \tag{2.25}$$

Given the existence of minimum variance unbiased estimator, the Cramér-Rao bound (2.19) saturates as

$$\mathrm{MSE}(\hat{\chi}) = \frac{1}{\mathcal{F} r}. \tag{2.26}$$

Combining (2.25) and (2.26) completes the proof. □

In the presence of phase-covariant noise, Theorem 1 quantifies the trade-off between the error probability in the estimation range and the severity of noise in higher-order GHZ states through achievable QFI for a noisy state. Figure 2.11 and 2.12 show that the

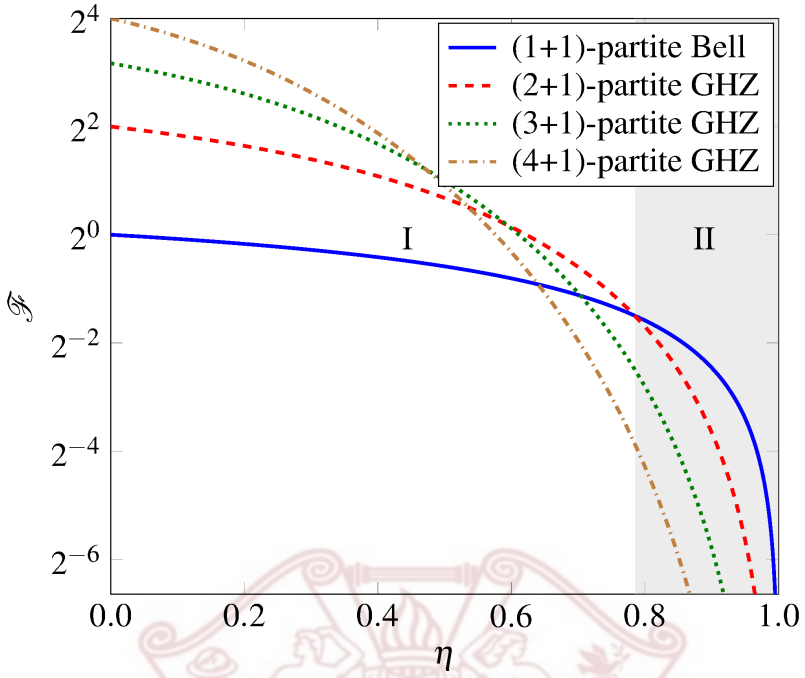


Figure 2.11: The QFI $\mathcal{F}$ of $(i+1)$-partite GHZ states, for i $\in \{1, 2, 3, 4\}$, as a function of noise parameter in amplitude damping noise. The shaded region corresponds to the case when only the shot-noise limited scaling is achievable and the shared Bell states are optimal for shift estimation.

QFI decreases monotonically with an increase in the noise strength, with steeper slopes for GHZ states with a higher number of qubits. Consequently, for a given nondegenerate noise model, there exists a GHZ state with an optimal number of qubits. After the identification of the optimal GHZ state, the accuracy requirements in terms of tolerable threshold ϵ and the probability of estimated shift to be outside this threshold determine the required minimum number of copies of the GHZ state. In a practical scenario, the estimate of noise is obtained by the purity measurement performed at the beginning of the LOS procedure. Figure 2.13 and 2.14 provide a graphical comparison of the QFI given the purity measurement. This figure signifies the importance of purity measurement not

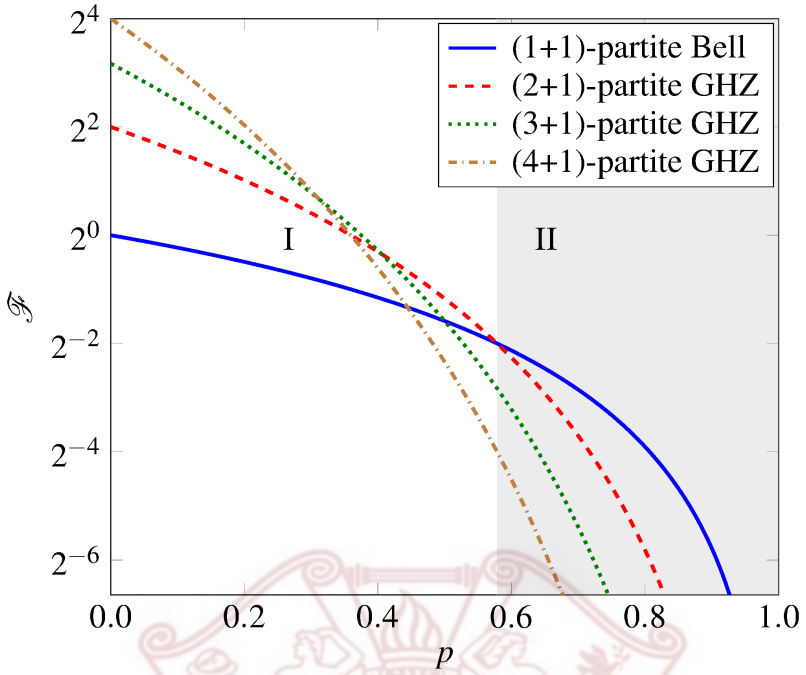


Figure 2.12: The QFI $\mathcal{F}$ of $(i+1)$-partite GHZ states, for i $\in \{1, 2, 3, 4\}$, as a function of noise parameter in depolarizing noise. The shaded region corresponds to the case when only the shot-noise limited scaling is achievable and the shared Bell states are optimal for shift estimation.

only in the characterization of new nodes in the DQN but also in the choice of optimal GHZ states for the LOS.

To illustrate the LO resyntonization, we consider the case where the maximum order of GHZ state available is 4+1; where $n_{\text{opt}} = 4$ qubits are sent to the node with LO shift and 1 ancilla qubit at a neighboring branch node. Figures 2.11, 2.12, 2.13, and Figure 2.14 compare the QFI (2.20) for the four states with varying numbers of entangled particles in shift estimation under phase-covariant noise. As evident from the figures, the absence of any noise provides Heisenberg scaling as the QFI obtained scales quadratically with the number of qubits ($n_{\text{opt}} = 4$) undergoing shift encoding unitary. Region-I in both figures

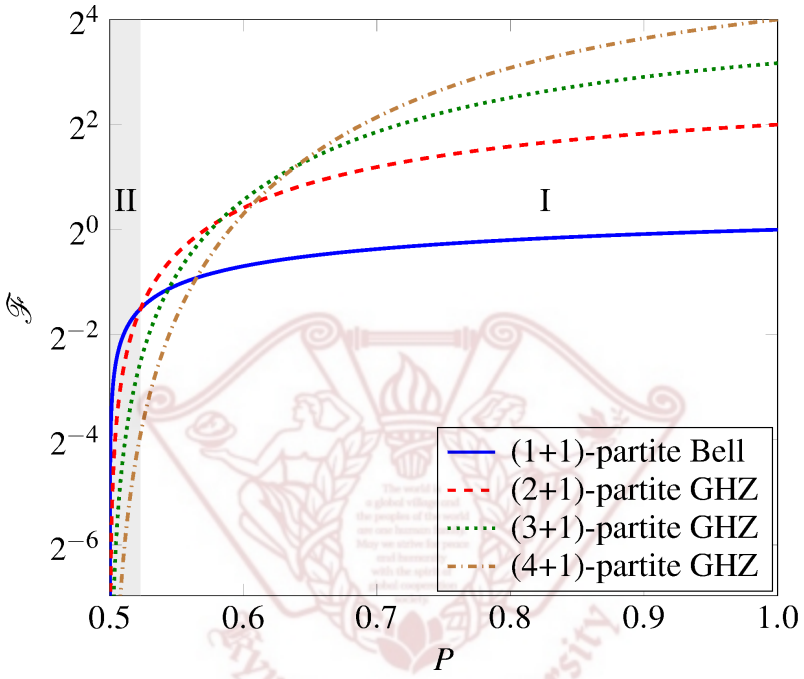


Figure 2.13: A comparison of different schemes in terms of the achievable QFI given the purity P, an observable of qubit noise, for $(i+1)$-partite GHZ states, i $\in \{1, 2, 3, 4\}$, under amplitude damping noise. The shaded region corresponds to the case when only the shot-noise limited scaling is achievable and the shared Bell states are optimal for shift estimation.

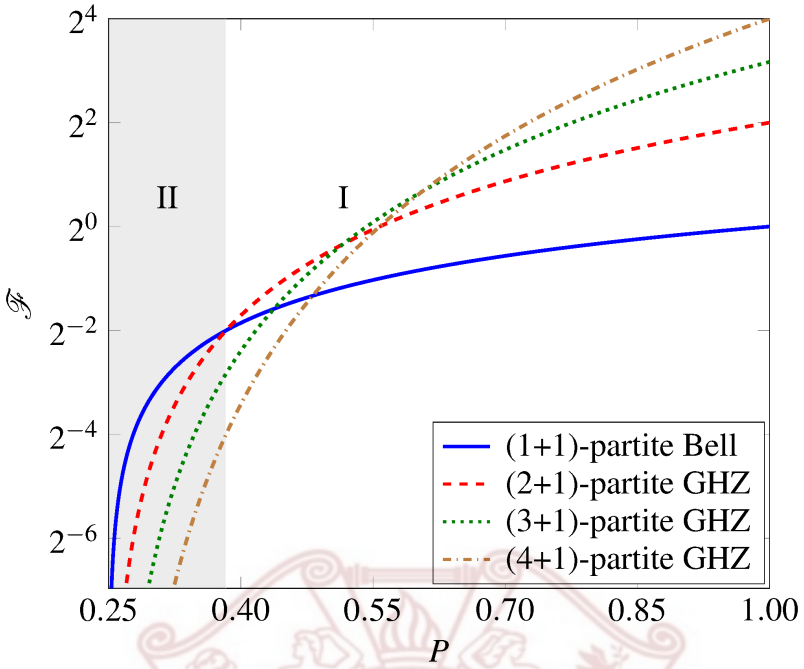


Figure 2.14: A comparison of different schemes in terms of the achievable QFI given the purity P, an observable of qubit noise, for $(i+1)$-partite GHZ states, i $\in \{1, 2, 3, 4\}$, under depolarizing noise. The shaded region corresponds to the case when only the shot-noise limited scaling is achievable and the shared Bell states are optimal for shift estimation.

shows how the higher-order entangled GHZ states are affected by the quantum noise and the configuration of parameter estimation depends on the measured P. In region-II, where the configuration used for shift estimation is the same as for the shift detection, the maximum achievable precision in shift estimate is shot-noise limited through the use of shared Bell state. Figures 2.11 and 2.12 also show that the advantage of higher-order GHZ states in precision vanishes in the regions of severe noise. Therefore, the purity measurement at the beginning of the protocol is crucial in finding the optimal number of qubits in the GHZ state. Once the shift χ has been estimated, the LO frequency is readjusted to syntonize the LOs and the corresponding clocks.

2.4 Conclusion

The distributed clock oscillator syntonization procedure presented in this paper allows precise and accurate syntonization in the operations of quantum communication and computation applications. For a centralized clock network [23], the presence of quantum noise at a single node may result in: 1) failure of the LOS procedure for the entire network if a single node loses its qubits and 2) decrease in the syntonization precision of all the nodes in case of a single node subject to phase-covariant noise. The DQN enables the distributed nodes to overcome these limitations of the centralized clock network by utilizing a distributed approach. One possible future direction is to extend the proposed scheme by combining it with the quantum error correction and fast quantum operations. This may allow achieving the Heisenberg limited precision even in the presence of local qubit noise.

Chapter 3

Counterfactual Secure Clock Synchronization

The recent advent of optical atomic clocks provides unprecedented challenges in clock synchronization to fulfill their potential for distributed computation networks. Classically, time synchronization between remote clocks is performed by time transfer laser links (otherwise known as Einstein's method) [17] or Eddington's slow clock transport [56]. Their quantum versions [25–28] employ non-classical resources to provide precision beyond the shot-noise limited precision achieved by their classical counterparts. In addition, quantum entanglement has provided the basis for a new paradigm of quantum clock synchronization (QCS), unparalleled in the classical domain [29]. Both Eddington [27] and entanglement-based [29] QCS protocols are inherently robust against the transmission delay associated with practical clock synchronization. However, these two QCS procedures substantially require shared phase reference [30–32]. The two-way exchange of clock qubit atoms (e.g., Cesium, Rubidium, Strontium) has been proposed to achieve synchronization without requiring a shared phase reference for Eddington-based QCS [28]. However, using atomic qubits for this QCS task is more challenging than photonic ones. Multiple two-way ex-

changes of atoms make this modified Eddington-based QCS protocol highly susceptible to channel noise. Meanwhile, it has been recently shown that [32] the entanglement-based QCS is feasible in the absence of shared phase reference using entanglement purification [57]. The trade-off associated with purification is the sacrifice of entangled pairs to improve the fidelity of the remaining pairs [57]. Both the channel noise and the absence of shared phase reference decrease the fidelity of the shared entangled state. Furthermore, the purification procedure works only for fidelity greater than 0.5. To counter these issues, the clocks involved need to be *a priori* synchronized to some extent, leading to additional practical constraints and overheads.

An adversary on the channel can impair all aforementioned QCS procedures by sabotaging information over the channel [58]. To counter this adversary, a separate quantum key distribution protocol has recently been utilized to encrypt time information that is subsequently used in the clock synchronization protocol [59]. Therefore, a clock synchronization protocol that provides i) sub-shot noise scaled precision, ii) robustness against channel noise, and iii) inherently secure against sabotage attacks by an adversary [58] iv) without requiring shared phase reference—becomes an intriguing prospect.

In this chapter, we present the theoretical framework of counterfactual secure clock synchronization, which requires no shared phase reference—as only one party performs quantum operations—while providing sub-shot noise scaled precision and robustness against noise. The proposed QCS protocol utilizes the counterfactual information transfer [52] to synchronize two distant clocks without transmitting any physical particle over the channel. Due to the counterfactual nature, the protocol is inherently secure against an adversary trying to sabotage the clock synchronization as well as robust against noise.

The remainder of this chapter is organized as follows. First, we provide the details of counterfactual communication. Then, we demonstrate the operation of conditional counterfactual rotation (CCR). Then, we provide the working of the CSCS scheme illustrating

its robustness in practical noisy channel conditions. Here on out, we discuss the precision and accuracy achieved in the CSCS scheme. Finally, we show that the CSCS scheme inherently fulfills the requirement of secure clock synchronization [58] by countering adversarial perturbations using the aid of only classical authenticated channel.

3.1 Counterfactual Communication

Throughout human history, information transfer between two distant locations required messengers. For the majority of human civilization, these messengers were actual people. In the last two centuries, information transfer has probably been revolutionized more than any other field. Now, we can communicate huge amounts of information at unprecedented rates through radio and microwave particles as messengers. Recently, a counter-intuitive information transfer method has been discovered which *does not require any messenger particles* between the two parties for information transfer [52, 60–69]. This method referred to as *counterfactual communication*, relies on the dynamic quantum Cheshire cat effect, wherein a controlled property of a particle can be modified at a location that the particle never visited [60]. To date, counterfactual communication has been utilized to transfer classical information, entanglement, and quantum information; which collectively are revolutionizing the next generation of information transfer through technologies like teleportation and super-dense coding to name a few [63, 70–75].

In recent years, direct counterfactual quantum communication has been demonstrated based on the quantum Zeno (QZ) effect, which enables distant parties to transfer information without transmitting any physical particle over the channel [52,63,65,66,68,73,75–78]. This unique property of the counterfactual quantum communication provides a distinctive paradigm to target the aforementioned requirements for secure, precise, and robust clock synchronization.

Counterfactual communication is a new mode of communication where information can

be transmitted without sending any physical particle over the channel [52,62,63,66,68,69, 74]. It relies on the dynamic quantum Cheshire-cat effect, wherein a controlled property of a particle can be modified at a location never visited by the particle itself [60]. Interaction-free measurements, which are used to infer the presence or absence of a particle without interacting with it, provide the basis for this counterfactual communication [79–83].

Direct counterfactual communication (DCC) is the first counterfactual protocol for particle-less communication [52]. It relies on the interaction-free measurement and chained QZ (CQZ) gates to transfer information without sending any photon over the channel [79–83]. This provides security and information concealing ability without requiring conventional quantum secure schemes [79–83]. The system setup consists of two cascaded Michelson interferometers, at one party (say Alice), acting on a photon's polarization degree of freedom. While an absorptive object (e.g., an electron) is available at the other party (say, Bob). The system has been provided in Fig. 3.1. In each cycle of the system, the polarization and path-controlled properties of a photonic wave function are modified based on the presence or absence of an absorptive object [60]. It is to be noted that although there is no information-carrying particle over the channel, counterfactual communication requires a quantum channel between the two parties on which the controlled property of the photon (but not the photon itself) interacts with the electron. The DCC and subsequent protocols based on DCC have been utilized for communication, remote computation, entanglement generation, and clock synchronization [73–75].

3.1.1 Counterfactual Conditional Rotation Gate

The DCC setup communicates classical information as follows: If the AO is present throughout the CQZ operation, the CQZ gate rotates the photon state by $M\theta_M$ where $\theta_M = \pi/(2M)$. When the AO is absent, the photon collapses to the initial state after M outer cycles. However, Alice can make its AO transition from absent to present state de-

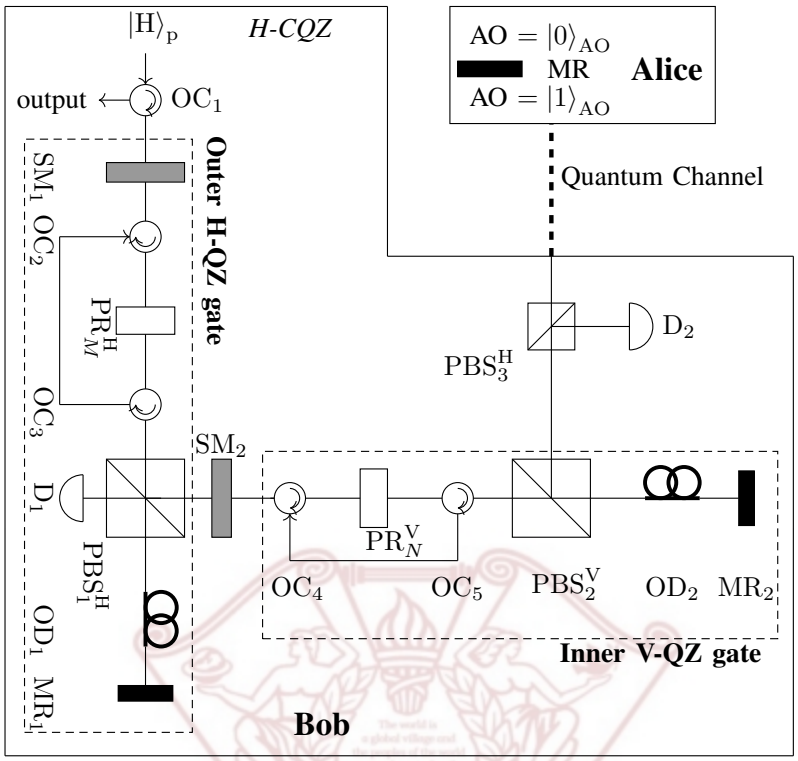


Figure 3.1: Chained quantum Zeno gate for DCC. On Bob's side, the optical elements are as follows: OC is an optical circulator, SM refers to the switchable mirror, PR represents the switchable polarization rotator, PBS corresponds to the polarization beam splitter, and OD and MR are optical delay element and mirror respectively.

pending on her local time. If her clock is not synchronized to Bob's clock, the AO becomes present sometime during the CQZ operation. In such a case, the CQZ gate gives partial rotation by an angle $\vartheta \leq M\theta_M$. We devise a CCR gate for desynchronization estimation (see Figure 3.2) and use its partial rotation to synchronize two clocks counterfactually.

Let the AO (Alice) be initially in the absence state $|0\rangle_A$, while the photon (Bob) is in

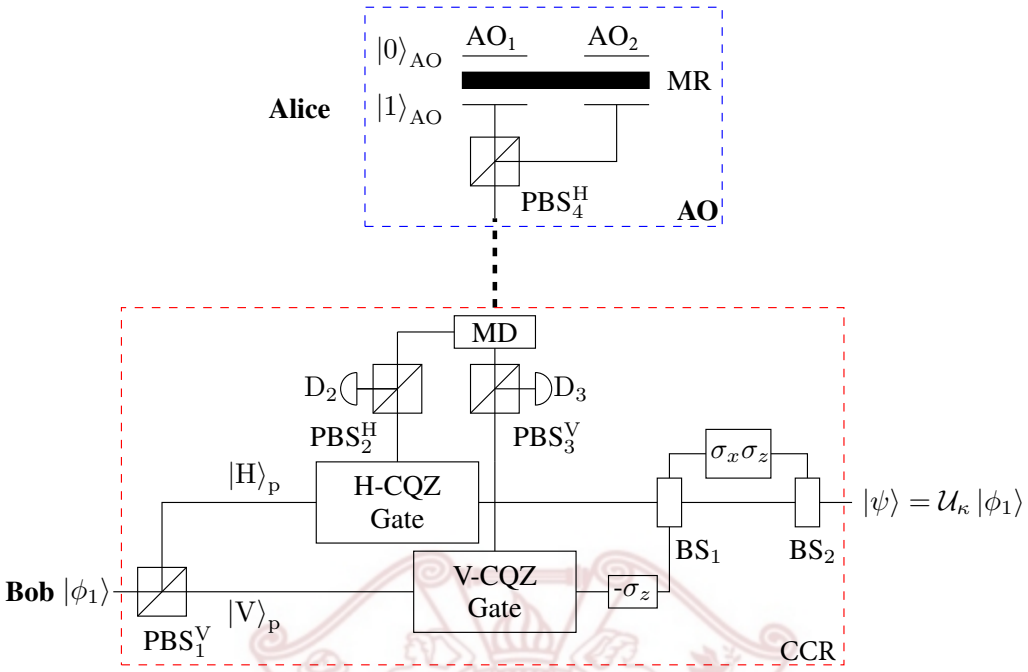


Figure 3.2: Counterfactual conditional rotation (CCR) architecture. MD stands for multiplexer/demultiplexer directing outgoing and incoming H(V) polarization components depending on the time instant they arrive. $AO_{1(2)}$ shows the AO for round-1 or 2.

the initial state

$$|\text{in}\rangle_B = \frac{1}{\sqrt{2}} \left(|H\rangle_B + |V\rangle_B \right), \tag{3.1}$$

where $|H\,(V)\rangle_B$ is the horizontal (vertical) polarization of Bob's photon. Bob starts the CCR operation by inputting his photon into the CCR gate as shown in Figure 3.2. To perform conditional rotation, Alice changes her AO state to the presence state $|1\rangle_A$ and keeps it for ζ remaining outer cycles of the CQZ operation where $\zeta \in [0, M]$ denotes the number of *active* outer cycles in the presence state $|1\rangle_A$ and $\zeta = 0$ stands for no transition such that the AO remains in the absence state $|0\rangle_A$ for all outer cycles. For this ζ-active transition, the pair of H- and V-CQZ$_{M,N}$ gates transform the initial state $|\text{in}\rangle_B$ of the

photon as

$$|\phi_1\rangle_{\mathrm{B}} = \frac{1}{\sqrt{2}}\left(\cos\zeta\theta_M\,|\mathrm{H}\rangle_{\mathrm{B}} + \sin\zeta\theta_M\,|\mathrm{V}\rangle_{\mathrm{B}}\right)|0\rangle_{\mathrm{C}} + \frac{1}{\sqrt{2}}\left(\cos\zeta\theta_M\,|\mathrm{V}\rangle_{\mathrm{B}} + \sin\zeta\theta_M\,|\mathrm{H}\rangle_{\mathrm{B}}\right)|1\rangle_{\mathrm{C}}\,, \tag{3.2}$$

where $|0\rangle_{\mathrm{C}}$ and $|1\rangle_{\mathrm{C}}$ show path information of the photon. Now, Bob applies $-\sigma_z$ on the photon component in the path state $|1\rangle_{\mathrm{C}}$ where σ_z is the single-qubit Pauli z operator. To rejoin the two paths of the photon, Bob applies the 50 : 50 beamsplitter (BS). BS_1 transforms the photon state as follows:

$$\begin{aligned}|\phi_2\rangle_{\mathrm{B}} =& \frac{1}{\sqrt{2}}\left(\cos\zeta\theta_M - \sin\zeta\theta_M\right)|\mathrm{H0}\rangle_{\mathrm{BC}} + \frac{1}{\sqrt{2}}\left(\sin\zeta\theta_M + \cos\zeta\theta_M\right)|\mathrm{V0}\rangle_{\mathrm{BC}} \\ &+ \frac{1}{\sqrt{2}}\left(\cos\zeta\theta_M + \sin\zeta\theta_M\right)|\mathrm{H1}\rangle_{\mathrm{BC}} + \frac{1}{\sqrt{2}}\left(\sin\zeta\theta_M - \cos\zeta\theta_M\right)|\mathrm{V1}\rangle_{\mathrm{BC}}\,.\end{aligned} \tag{3.3}$$

The photon component in the path state $|1\rangle_{\mathrm{C}}$ undergoes the Pauli rotation $\sigma_x\sigma_z$ and is combined with the other photon component using BS_2, where σ_x is the single-qubit Pauli x operator. Then, we have the output photon as

$$\begin{aligned}|\mathrm{out}\rangle_{\mathrm{B}} &= \frac{1}{\sqrt{2}}\left(\cos\zeta\theta_M - \sin\zeta\theta_M\right)|\mathrm{H}\rangle_{\mathrm{B}} + \frac{1}{\sqrt{2}}\left(\cos\zeta\theta_M + \sin\zeta\theta_M\right)|\mathrm{V}\rangle_{\mathrm{B}} \\ &= \boldsymbol{R}\left(\zeta\theta_M\right)|\mathrm{in}\rangle_{\mathrm{B}}\,,\end{aligned} \tag{3.4}$$

where

$$\boldsymbol{R}\left(\theta\right) = \begin{bmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{bmatrix} \tag{3.5}$$

is the rotation obtained by the CCR gate with the ζ-active transition of Alice's AO. Note that the CCR angle $\zeta\theta_M \in \mathcal{A}$ is proportional to ζ, i.e., the number of active outer cycles in the presence state $|1\rangle_{\mathrm{A}}$ during the operation, where $\mathcal{A} = \{0, \theta_M, 2\theta_M, \ldots, M\theta_M\}$ is the set of $M+1$ CCR angles.

3.1.2 CCR-QCS Protocol

We consider that Alice acts as a server clock and Bob as a client clock that wants to remove ΔT-time desynchronization with the server clock where

$$|\Delta T| \leq \Delta T_{\max}. \tag{3.6}$$

Here, positive and negative values of ΔT represent lagging and leading times of the client clock, respectively, and the maximum desynchronization $\Delta T_{\max}$, known *a priori*, is a function of clock stabilization. Let $T_{\rm rt}$ be photon's round-trip time between Alice and Bob. Then, we set $\Delta T_{\max}$ within the CQZ duration $MNT_{\rm rt}$, i.e., $\Delta T_{\max} \leq MNT_{\rm rt}$ for the CCR operation with H(V)-CQZ$_{M,N}$ gates. The CCR gate is only able to encode the information of $|0\rangle_{\rm A} \rightarrow |1\rangle_{\rm A}$ transition. For $|1\rangle_{\rm A} \rightarrow |0\rangle_{\rm A}$, the CCR gate does not change the input state [76], leading to $\zeta = 0$. Hence, Alice and Bob utilize two CCR gates to capture the $|0\rangle_{\rm A} \rightarrow |1\rangle_{\rm A}$ transition for both the cases of lagging and leading client clocks as shown in Figure 3.3. In each CCR gate, Bob inputs K batches of L noninterfering photons where all L photons in each batch are input to the CCR gate at the same time due to no interference between them (see Figure 3.4). Note that as can be seen from (3.4), the CCR angle of the output photon depends on the active outer-cycle number ζ. Hence, the detectable time resolution of desynchronization is equal to one outer-cycle duration $NT_{\rm rt}$ attained by using a single batch of photons for the CCR operation. For a high synchronization resolution, K photon batches are input to the CCR gate successively with time delay (resolution)

$$T_{\rm sep} = \frac{NT_{\rm rt}}{K}. \tag{3.7}$$

In the prior classical handshake, Alice and Bob share the start time t_l of the CCR gate-l ($l = 1, 2$) and the maximum desynchronization $\Delta T_{\max}$. Let $t_{\rm A}$ and $t_{\rm B}$ be clocks of Alice and Bob, respectively. We also consider that for the kth batch in the CCR gate-l,

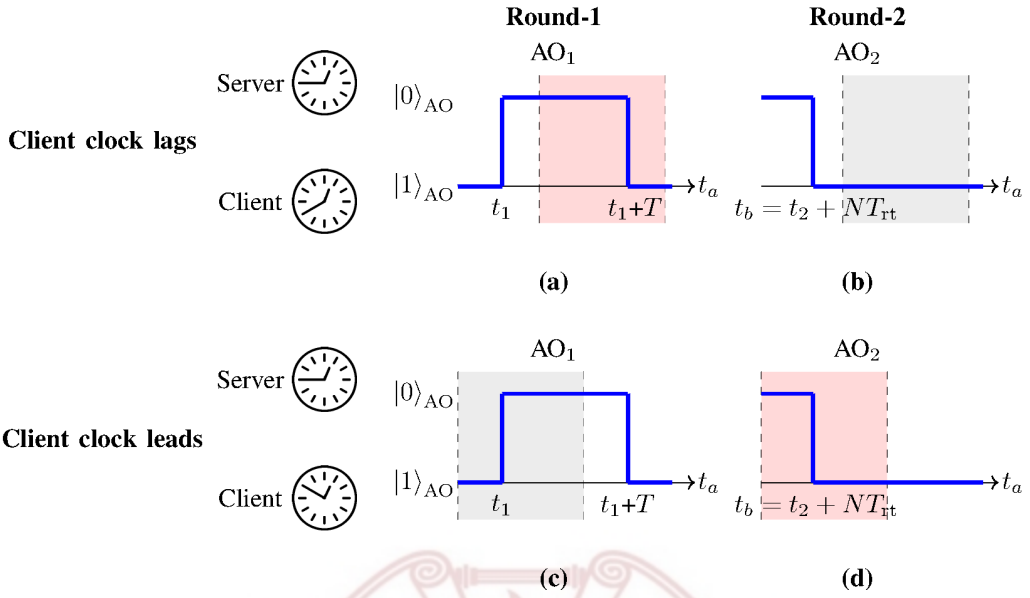


Figure 3.3: Four scenarios of the CCR operation for CSCS. The shaded region in each scenario shows the duration of AO-photon component interactions. We obtain desynchronization information through **(a)** and **(d)** scenarios due to $|0\rangle_{\mathrm{AO}} \rightarrow |1\rangle_{\mathrm{AO}}$ transition. Meanwhile, CCR does not modify the input state for **(b)** and **(c)** scenarios.

$L_{l,k}$ photons remain successfully, whereas other $(L - L_{l,k})$ photons are absorbed by Alice's AO or discarded at the detectors in the CCR gate due to traveling over the channel. The absorbed or discarded photons will therefore be removed from a further synchronization mechanism. To devise the CCR-QCS protocol under the ideal conditions, Alice (server clock) initializes her two AO states in $|10\rangle_{\mathrm{A}} = |1\rangle_{\mathrm{AO}_1} |0\rangle_{\mathrm{AO}_2}$ as the presence and absence states for the first and second CCR gates, respectively. Then, Alice and Bob take the following steps.

1. At time $t_{\mathrm{A}} = t_0$, Alice flips her AO_1 state from $|1\rangle_{\mathrm{AO}_1}$ to $|0\rangle_{\mathrm{AO}_1}$ and keeps it in the absence state $|0\rangle_{\mathrm{AO}_1}$ for time T required to complete CCR operation for all K

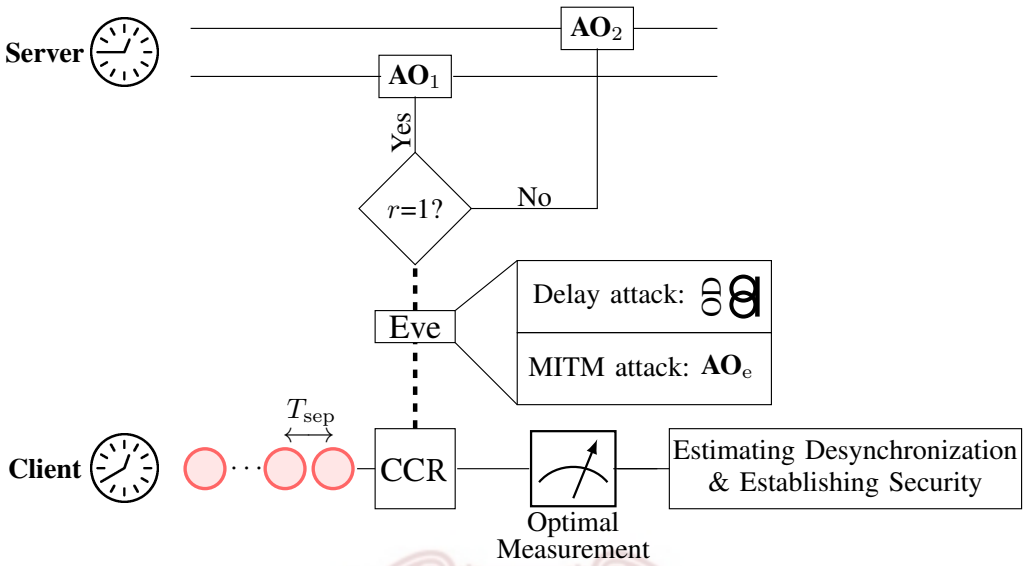


Figure 3.4: Schematics of the CSCS framework. Photons batches represented as pink circles undergo unitary transformation inside CCR conditioned on the instant when the AO appears on Alice's side.

photon batches

$$T = MNT_{\rm rt} + (K-1)\,T_{\rm sep}. \tag{3.8}$$

Alice keeps her AO_2 in the state $|0\rangle_{\mathrm{AO}_2}$ till $t_{\rm A} = t_0 + (K-1)\,T_{\rm sep}$. At this time, Alice flips AO_2 from $|0\rangle_{\mathrm{AO}_2}$ to $|1\rangle_{\mathrm{AO}_2}$ and keeps AO_2 in the presence state $|1\rangle_{\mathrm{AO}_2}$ for the protocol. At time $t_{\rm A} = t_0 + T$, Alice reflips AO_1 from $|0\rangle_{\mathrm{AO}_1}$ back to $|1\rangle_{\mathrm{AO}_1}$. That is, Alice starts the protocol by changing her AO states as $|10\rangle_{\rm A} \to |00\rangle_{\rm A} \to |01\rangle_{\rm A} \to |11\rangle_{\rm A}$ at time $t_{\rm A} = t_0$, $t_{\rm A} = t_0 + (K-1)\,T_{\rm sep}$, and $t_{\rm A} = t_0 + T$ (see Figure 3.3).

2. Bob starts the protocol at his corresponding time $t_{\rm B} = t_0$ and inputs the kth batch of L noninterfering photons into each CCR gate at time $t_{\rm B} = t_0 + (k-1)\,T_{\rm sep}$ where each of L photons is in the initial state $|\mathrm{in}\rangle_{\rm B}$. The CCR gate-$l$ transforms each of

$L_{l,k}$ output photons in the kth batch as follows:

$$|\text{out}_{l,k}\rangle_{\text{B}} = \boldsymbol{R}\left(\zeta_{l,k}\theta_M\right)|\text{in}\rangle_{\text{B}} \tag{3.9}$$

where the output photons for the kth batch undergo the CCR angle $\zeta_{l,k}\theta_M \in \mathcal{A}$ depending on the $\zeta_{l,k}$-active transition of Alice's AO_l due to desynchronization of the client clock (Bob). Let $\boldsymbol{\zeta}_l = (\zeta_{l,1}, \zeta_{l,2}, \ldots, \zeta_{l,K})$ be sequences of CCR angle indices. Then, since all K batches are input to the CCR gates within one outer-cycle duration, the sequences $\boldsymbol{\zeta}_l$ are constant or monotonically increasing with integers in $[0, M]$.

- **CCR Gate-1**: If the client clock lags the server clock, then the CCR index $\zeta_{1,k}$ for the CCR gate-1 increases with the desynchronization of the lagging client clock and $\zeta_{1,k} = M$ for the maximum lagging desynchronization. Note that if the client clock is synchronized with or leads the server clock, $\zeta_{1,k} = 0$ for all $k \in [1, K]$, which prevents to detect leading desynchronization using the CCR gate-1.
- **CCR Gate-2**: If the client clock leads the server clock, then the CCR index $\zeta_{2,k}$ for the CCR gate-2 decreases with the desynchronization of the leading client clock and $\zeta_{2,k} = 0$ for the maximum leading desynchronization. Note that if the client clock is synchronized with or lags the server clock, $\zeta_{2,k} = M$ for all $k \in [1, K]$, which prevents to detect lagging desynchronization using the CCR gate-2.

3. After the CCR operation, Bob applies the optimal square root measurement (SRM) [84] to determine the CCR angle of each output photon. Since the set of possible output states in (3.9) forms the geometrically uniform symmetry (GUS), the optimal SRM enables to achieve the minimum error discrimination using measurement operators exhibiting the same GUS as evident in Figure 3.5 [84,85]. Let $\{\Pi_0, \Pi_1, \cdots, \Pi_M\}$

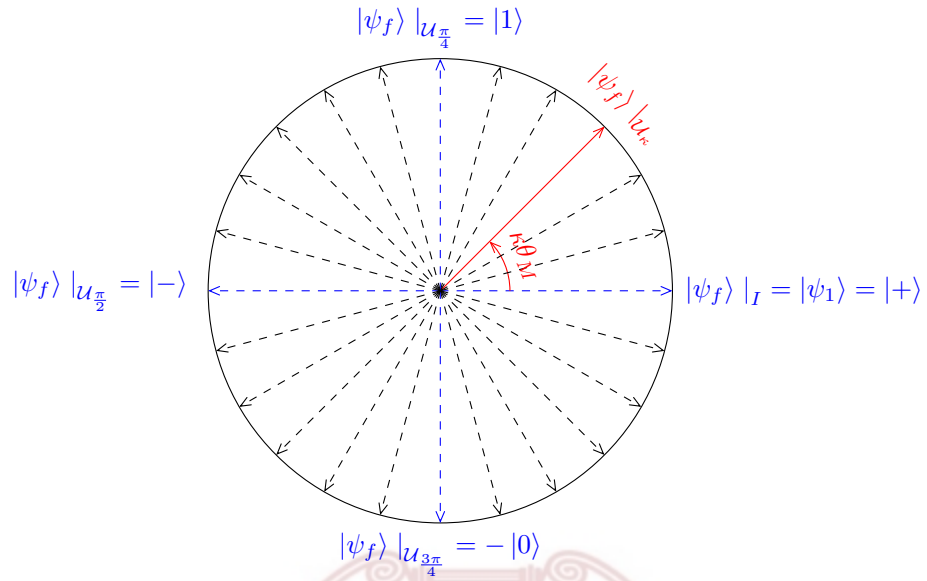


Figure 3.5: Geometrically uniform symmetry (GUS) of the possible CCR output states on the X-Z axis cross-section of the Bloch sphere. The two vectors normal to the plane are for Eve detection.

be the set of elementary measurement operators for this optimal SRM where

$$\Pi_i = \boldsymbol{R}\left(i\theta_M\right)|\text{in}\rangle_{\text{B}}\langle\text{in}|\,\boldsymbol{R}\left(i\theta_M\right) \tag{3.10}$$

is the measurement operator corresponding to the ith CCR angle $i\theta_M \in \mathcal{A}$. Then, Bob estimates the CCR index $\hat{\zeta}_{l,k}$ for the kth batch using $L_{l,k}$ output photons that successfully complete the CCR operation to empirically find

$$\zeta_{l,k} = \underset{i\in[0,M]}{\arg\max}\,\langle\text{out}_{l,k}|_{\text{B}}\,\Pi_i\,|\text{out}_{l,k}\rangle_{\text{B}}\,. \tag{3.11}$$

For all K batches, Bob determines two sequences $\hat{\boldsymbol{\zeta}}_l = \left(\hat{\zeta}_{l,1}, \hat{\zeta}_{l,2}, \ldots, \hat{\zeta}_{l,K}\right)$ of the CCR estimates from measurement outcomes for two CCR gates. By definition, the sequences $\hat{\boldsymbol{\zeta}}_l$ are estimated to be constant or monotonically increasing with with

integers in $[0, M]$. For example, $\hat{\boldsymbol{\zeta}}_l = \mathbf{0}_K$ (all-zero sequence of length K) and $\hat{\boldsymbol{\zeta}}_2 = M\mathbf{1}_K$ (all-M sequence of length K) imply that Bob is synchronized with Alice.

4. Using two sequences $\hat{\boldsymbol{\zeta}}_l$ of CCR estimates, Bob determines his desynchronization time with the server clock as follows:

$$\Delta\widehat{T} = \Delta\widehat{T}_1 + \Delta\widehat{T}_2 \tag{3.12}$$

where the lagging and leading desynchronization estimates $\Delta\widehat{T}_1$ and $\Delta\widehat{T}_2$ are given by

$$\Delta\widehat{T}_l = \alpha_l T_{\text{sep}} + \left(\hat{\zeta}_{l,1} - (l-1)\, M\right) N T_{\text{rt}} \tag{3.13}$$

and α_l is the number (multiplicity) of elements unequal to $\hat{\zeta}_{l,1}$ in the sequence $\hat{\boldsymbol{\zeta}}_l$. Note that the positive and negative signs of desynchronization estimate $\Delta\widehat{T}$ represent the lagging and leading times, respectively.

3.1.3 Precision in CCR-QCS

Due to the discretization of desynchronization, there is inherent uncertainty in the desynchronization estimate $\Delta\widehat{T}$, where the true value ΔT lies within $\pm T_{\text{sep}}/2$ of the estimated time $\Delta\widehat{T}$. Without the *a priori* information, we assume the uniform distribution of $\Delta\widehat{T}$ in this interval, and the variance (or mean square error) of $\Delta\widehat{T}$ is given as

$$\begin{aligned} \text{Var}\big[\Delta\hat{T}\big] &= \frac{T_{\text{sep}}^2}{12} \\ &\propto \frac{1}{K^2}. \end{aligned} \tag{3.14}$$

From (3.14), it can be clearly seen that the variance of $\Delta\widehat{T}$ scales quadratically with the number of batches (independent of the number of photons in each batch), thus achieving *Heisenberg scaling*.

In practice, the synchronization resolution T_{sep} can be limited by the generation rate of the single-photon source. The maximum achievable generation rate of an ideal photon

source depends on the *wavepacket duration* ΔD of each photon [86]. Without loss of generality, we can assume that photons are in Fourier-transform-limited Gaussian spectral-temporal mode [87], leading to the following relation between the temporal duration ΔD and the photon frequency bandwidth ΔS [88]:

$$\Delta D \Delta S = 1. \tag{3.15}$$

For instance, spontaneous parametric down-conversion sources are readily available which generate single photons at 1550-nanometer (nm) center wavelength and 300 GHz frequency bandwidth [89], which limits the resolution T_{sep} to 3.33 picoseconds. Recently, a number of practical techniques have been proposed for ultrafast single-photon generation [90–93].

3.1.4 Accuracy in CCR-QCS

From (3.13), time desynchronization estimate of the proposed protocol depends on the correct identification of the $\zeta_{l,k}$. As discussed earlier, the output states and therefore the optimal measurement operators have the same GUS symmetry (See Figure 3.5). For this case, the correct decision probability P_{corr} to correctly identify $\zeta_{l,k}$ is given as [84, 85]

$$P_{\text{corr}} = \left(\frac{1}{M+1} \sum_{\zeta=0}^{M} \sqrt{\sum_{y=0} \exp\left\{-\iota 2\pi \zeta y/M\right\} \cos\left(y\theta_M\right)} \right)^2. \tag{3.16}$$

In practice, the relative frequency of the measurement outcomes approaches corresponding outcome probabilities under the asymptotic limits. Hence, we can empirically estimate $\zeta_{l,k}$ through (3.11). In this case, the estimation error $\Delta\zeta_{l,k} = \zeta_{l,k} - \hat{\zeta}_{l,k}$ approaches to zero as the number of photons $L_{l,k}$ increases; which leads to the accurate estimate of ΔT for a given precision.

Practical imperfections like fiber optic delays may reduce the accuracy of the CCR-QCS because the output state will drift away from the ideal output state leading to error in the identification of $\zeta_{l,k}$. The transmission channel delay of the photon component in

the inner interferometer may lead to a mismatch between two arms in the path DOF. Operationally, this will induce a rotation about the Z-axis in the Bloch sphere on the components in the inner interferometer of H(V)-CQZ through

$$\boldsymbol{U}_{\mathrm{H}_{\phi_b}}\left(\boldsymbol{U}^{\dagger}_{\mathrm{V}_{\phi_b}}\right) = \begin{pmatrix} e^{\iota\phi_b/2} & 0 \\ 0 & e^{-\iota\phi_b/2} \end{pmatrix}, \tag{3.17}$$

where ϕ_b is the rotation angle due to the change in channel length. If ϕ_b is small enough so that the practical output state is still closest (in trace distance) to the ideal output state, accuracy will not be affected for sufficiently large $L_{l,k}$. Otherwise, channel delay will lead to an inaccurate estimation of ΔT.

Recent practical implementations of counterfactual schemes with $M = 3$ and $N = 8$ have achieved an effective arm mismatch of the order of nanometers. Consequently, it is possible to bound the rotation to be of order $\phi_b = \delta T_c 2\pi f \sim 4.05 \times 10^{-3}$ radians by utilizing photons of telecom wavelength 1550 nm and natural frequency $f \sim 193.55$ THz since the output state will remain closest (in trace distance) to the corresponding ideal state as shown in Figure 3.6 for uniformly distributed random $\phi_b \mod 2\pi < |0.1|$ in each channel transmission. Therefore, we can accurately estimate $\zeta_{l,k}$. In classical and quantum Einstein synchronization methods, a substantial part of the uncertainty in desynchronization estimate is the variation in transmission time. This variation in transmission time effects cannot be mitigated without introducing additional pre-and post-processing. In the *Security of CSCS*, we show the inherent ability of CSCS to detect channel delay attacks if the adversary's channel delay attack induces phase > 0.1.

3.1.5 Security of CSCS

An adversary (Eve) may attempt to sabotage the clock synchronization procedure by modifying the information exchanged between the legitimate parties. For any clock synchronization procedure to be secure against adversarial parties, it needs to detect two types

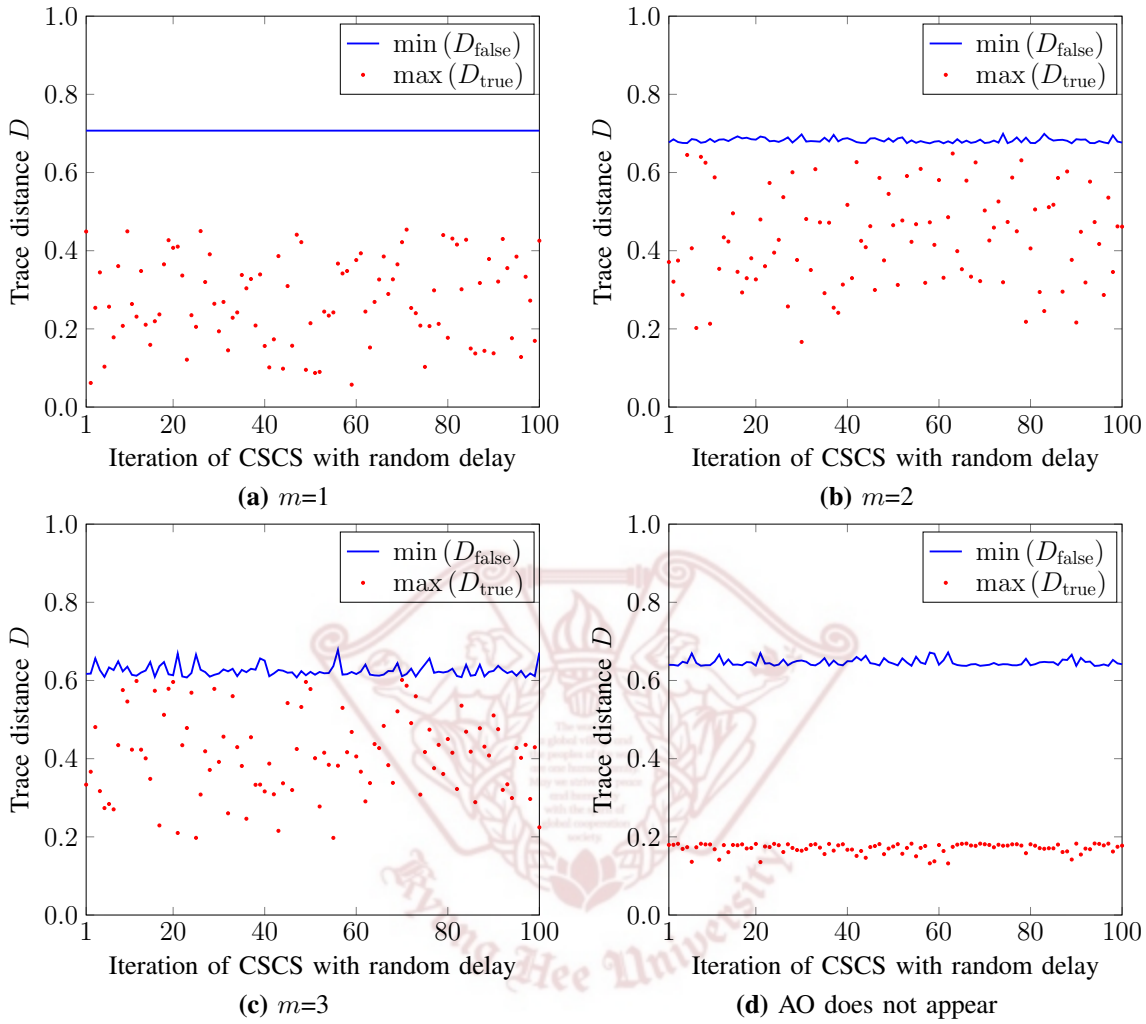


Figure 3.6: Trace distance of the practical output states (for each m and n) from all the possible cases in the absence of noise, due to random channel delay time δT_c. $\max(D_{\text{true}})$ is the maximum trace distance of practical output states (for each iteration) from the expected output in noiseless case while $\min(D_{\text{false}})$ is the minimum trace distance from all other possible output states in the noiseless case; for the practical CSCS setup with a photon of telecom wavelength 1550 nm and thus $f \sim 193.55$ THz, Eve induced channel delay $4.05\times10^{-3} < \phi_b \mod 2\pi < |0.1|$, and M=3 and N=8. Since the noisy output states stay closest to the output state for the noiseless case, we can decrease error probability by increasing K. If AO is present throughout CCR operation, the channel delay will not affect CSCS.

of attacks, namely A) man-in-the-middle (MITM) attack and B) time delay attack [58]. Here we show that the CSCS is inherently secure against these two attacks.

Man-in-the-middle attack: Eve can utilize its own absorption object AO_e to employ MITM (Figure 3.4). The most general type of MITM attack is the intercept-and-resend attack, where the adversary intercepts the communicating particles and sends the same or newly prepared particles to the receiving party after some modification [59]. However, due to the counterfactual nature of CSCS, the photons providing time data do not enter the channel. Therefore, the adversary Eve cannot access the entire quantum system of each signal particle, but only part of the quantum system. Hence, intercept-and-resend attacks cannot sabotage the CSCS because *particles* are not captured.

Eve can employ a more specific MITM approach to sabotage the CSCS scheme by taking over the role of Alice for the incoming signals from Bob. For this case, she has to match the exact channel length to the original channel between Alice and Bob. If she does not exactly match the channel length, this will become a type of time delay attack, which will lead to her identification as discussed in the *Channel delay attack*. Here, we assume that Eve has matched the channel length, and thus Bob is oblivious to her presence. Then, Eve can use her own AO_e and mirror MR_e to provide the wrong desynchronization estimate to Bob. We recall that the essence of counterfactual protocols is to transmit information without sending any particles into the channel. However, there is a non-zero probability that some particles will end up in the channel. These particles do not carry any information and are absorbed at either of the communicating parties. We utilize the information about these ℓ absorbed photons and classical communication to inherently provide security against this MITM attack. We can further increase the security of the scheme by employing decoy photons intentionally injected into the channel. The number of decoy photons d depends on the security of the CSCS specified by the required minimum probability of Eve's detection $P_S \in [0, 1)$. P_S depends on the probability of a photon going

into the channel and d, where the former itself is based on M and N. Based on the P_S, Bob chooses the number of decoy photons d and counters this attack through two cases.

- Case-1: Absorbed photons that were intended for counterfactual clock synchronization. There are two scenarios for such photons:

  A) Photon is absorbed by AO at Alice's end: After CSCS, Bob sends Alice the time $t_o^{a_e}$ when the photon component should have had the last interaction with AO, over the classical channel [59]. Superscript a_e indicates that Bob has translated this time according to the synchronization information between him and Alice but may actually be due to the synchronization with Eve. If Alice did not absorb a photon at $t_o^{a_e} - \sum_{i=0}^{NM-1} i2T_c$, the presence of Eve at the channel is established.

  B) Photon is absorbed at Bob's end after the pth outer cycle: Bob sends Alice the time $t_p^{a_e}$ when photon should have last interaction with AO and verifies if Alice absorbed a photon at $t_p^{a_e} - \sum_{i=0}^{N-1} i2T_c$. If Alice's AO was present throughout the pth outer cycle, and Alice did not absorb the photon, they conclude that Eve is executing the MITM attack. In all other cases, the presence of Eve cannot be detected.

- Case-2: To enhance security, d decoy photons are directly inserted into the channel. For increasing the probability of Eve detection, we directly inject d decoy photons into the channel. The decoy photons are equally distributed between $K \cdot MN$ AO-photon component interaction time-slots.

For the $K\gamma$ photons intended for desynchronization estimation, the expected *a priori* of Eve's detection is $P_{S_{MN}} = 1 - [1 - P_{S_{MN}}(|1\rangle_{\mathrm{AO}})]^{K\gamma}$. From the *Methods* section,

$$P_{S_{MN}}(|1\rangle_{\mathrm{AO}}) = \frac{1}{(MN)^2}\frac{1}{(K+1)}\sum_{j=1}^{MN} jP_{\mathrm{poc}_j}\left(\frac{K}{2MN}(1-2j) + \frac{1}{2}(2K+1)\right), \tag{3.18}$$

where $P_{\text{poc}_j} = (1 - \lambda_{n,m}\,|)$ is the probability of a photon ending up in the channel given AO present and $\lambda_{n,m}$ is the probability of a photon not absorbed.

Similarly, the probability of Eve detection due to the decoy photons is $P_{S_d} = 1 - [1 - P_{S_d}(|1\rangle_{\text{AO}})]^d$. However, since the decoy photons are directly injected into the channel, $P_{\text{poc}_j} = 1$. Therefore,

$$P_{S_d}(|1\rangle_{\text{AO}}) = \frac{1}{(MN)^2}\frac{1}{(K+1)}\sum_{j=1}^{MN} j\left(\frac{K}{2MN}(1-2j) + \frac{1}{2}(2K+1)\right). \tag{3.19}$$

The *a prori* probability of Eve detection is therefore, $P_S = 1 - [(1 - P_{S_{MN}})(1 - P_{S_d})]$.

Channel delay attack: From Figure 3.4, the second attack at Eve's disposal is the time-delay attack, wherein, Eve utilizes a change in the effective path length of the transmission channel to try and sabotage CSCS [59]. By counterfactually transmitting the state of Alice, the information about Eve's sabotage attack through channel delay is encoded into the output state of the photon. Under the channel transmission delay induced by Eve, the photon component in the inner interferometer undergoes the map

$$\boldsymbol{U}_{\hat{\phi}_{e\text{H}}} = \boldsymbol{U}^{\dagger}_{\hat{\phi}_{e\text{V}}} = \begin{pmatrix} e^{\iota\phi_e/2} & 0 \\ 0 & e^{-\iota\phi_e/2} \end{pmatrix}. \tag{3.20}$$

As explained earlier in the *Noise analysis*, the CSCS is robust against such an attack if it leads to a phase $< \phi_{\min} \mod 2\pi$, where $\phi_{\min}$ is the minimum phase for which accuracy is not affected and is a function of M, N and desynchronization. Here we show that CSCS has a further inherent ability to *detect* Eve's channel delay attack beyond this noise level.

If the AO is present throughout the CCR operation, any channel delay induced by Eve or otherwise does not affect the synchronization. This is because the AO absorbs any component going in the channel while the remaining wave components all reside at the client clock's end. However, for the rest of the cases, Eve does affect the CSCS by introducing a circular polarization component proportional to κ (the outer cycle in which

AO appears) in the output state. To detect this channel delay attack, Bob measures a subset ℓ_d of γK photons in Y basis and calculates the relative frequencies $\left|\bar{P}_{\rm e}\right|_{\ell_d}$ of two outcomes. Both of these outcomes are equiprobable in the ideal case, i.e., when there is no channel delay. In the practical implementation based on Cao *et al.* [65] considering $M = 3$ and $N = 8$, the maximum difference between the probabilities of two outcomes $|P_{\rm e}|$ in the absence of Eve is $|P_{\rm e}|_{\rm min} = 4.0244 \times 10^{-4}$. Any delay introduced by Eve that leads to $|P_{\rm e}| > |P_{\rm e}|_{\rm min}$, indicates the presence of Eve. In experimental setups, Alice and Bob need to calibrate the channel depending on the practical considerations and limitation to fix $|P_{\rm e}|_{\rm min}$. Such a calibration includes the uncertainties in the length of fiber optic between the two parties and in any optical element delays. The practical details of Eve detection by identifying the relative frequency difference $\left|\bar{P}_{\rm e}\right|_{\ell_d} > |P_{\rm e}|_{\rm min}$ at Significance $\mathrm{P} < 0.05$ [94] for channel delay attack are provided in the *Methods* section.

Recently, quantum correlations have been used to inherently provide security against symmetric delay attacks and with some modification (involving polarization entanglement and the Bell's inequality check) counter intercept and resend attack [95]. However, unlike CSCS, this procedure is susceptible to asymmetrical delays [96].

3.2 Methods

3.2.1 Unitary Identification

In CCR-QCS, the unitary identification plays an important role to estimate the desynchronization between Alice and Bob. As shown in Figure 3.5, the $M + 1$ output states of the CCU operation have the GUS. For GUS, the square root measurement is the optimal measurement setup with GUS symmetry same as possible output states. The single-qubit operators $\{\Pi_0, \Pi_1, ..., \Pi_Y\}$ for square root measurement are defined as

$$\Pi_y = |\phi_y\rangle \langle\phi_y| . \tag{3.21}$$

where $|\phi_y\rangle$ are the measurement vectors with symmetry operator same as the output states ($|\phi_y\rangle = \mathcal{U}_y |\phi_1\rangle = e^{-i(y\theta_M)\sigma_y} |\phi_1\rangle$). For this case, the correct decision probability in unitary discrimination is [97]

$$P_{\text{succ}} = \left(\frac{1}{M+1} \sum_{\kappa=0}^{M} \sqrt{\sum_{y=0} e^{-\iota 2\pi\kappa y/M} \cos(y\theta_M)} \right)^2, \tag{3.22}$$

To increase the P_{succ} and hence the error in estimated $\zeta_{l,k}$, we use $L_{l,k} \gg 1$ photons in each batch of photons.

3.2.2 Probability of a photon never in the channel

In the above sections, we demonstrated the time desynchronization estimation using counterfactual quantum communication. However, the success of desynchronization estimation is limited by the *probability that the photon is absorbed in CCR operation.* These photons though not useful for desynchronization estimation come in handy for achieving security against the sabotage attack. To determine the probability $\lambda_{n,m}$ that the particle is never found in the transmission channel in each round of the CCR operation, we consider that the AO appears in the nth inner cycle of the mth outer cycle. The $\lambda_{n,m}$ is given as

$$\lambda_{n,m} = a \times b \times c, \tag{3.23}$$

where a, b and c are the probabilities that the photon is not absorbed upto $(m-1)$th outer cycles, mth outer cycle and during subsequent $M-m$ outer cycles, respectively. The a, b and c for a given m and n are defined as

$$a = \cos^{m-1}\theta_M, \tag{3.24}$$

$$b = \left(1 - \sin^2\theta_M \sin^2 n\theta_N\right) \left(1 - \sin^2\theta_M \sin^2\theta_N\right)^{N-n} \left(1 - \sin^2\theta_M \sin^2\theta_N\right)^{2N}, \tag{3.25}$$

$$c = \prod_{i=m+1}^{M} \left[1 - \sin^2(M-i+1)\theta_M \sin^2\theta_N\right]^{2N}. \tag{3.26}$$

As M and N increase, the probability of a photon ending up in the channel decreases. Consequently, the number of photons that go in the channel and are used in the security is reduced.

3.2.3 Probability of AO present for a MITM attack

For detecting the MITM attack, photons that were absorbed by the AO during the CCR operation are used. To enhance security d decoy photons may also be used. For both of these, Eve detection depends on the probability of AO present when a photon ends up in the channel. The probability of AO appearing in a particular mth outer and nth inner cycle is $\frac{MN-n+1-\sum_{i=1}^{m-1}(iN)}{MN}$. Each of the K batches of photons undergoes a unitary encoding based on the magnitude of desynchronization between the clocks. For the 1st batch, AO is always absent except for the maximum desynchronization case; wherein the batch interacts with AO present during Mth outer and Nth inner cycle. Hence, the probability of AO present when interaction occurs is $\frac{1}{MN} \cdot \frac{1}{K+1}$. For the last ($K$th) batch, this probability is $\sum_{j=1}^{MN} \frac{MN-j+1}{MN} \cdot \frac{K}{MN(K+1)}$. For a specific case of m and n, $\lambda_{n,m}$ in (3.23) provides the probability of a photon never ending up in the channel for each batch. Assuming the photons that end up in the channel are uniformly distributed over the K batches, the probability of AO present given a photon ends up in the channel for photons $P(|1\rangle_{\mathrm{AO}}) \,|\, \mathrm{poc}$ is

$$P(|1\rangle_{\mathrm{AO}}) \,|\, \mathrm{poc} = \frac{1}{(MN)^2} \frac{1}{(K+1)} \sum_{j=1}^{MN} j \left(\frac{K}{2MN} (1-2j) + \frac{1}{2} (2K+1) \right). \tag{3.27}$$

Since decoy photons are directly injected into the channel, therefore, probability of Eve detection for decoy photons is $P_{S_d} = P(|1\rangle_{\mathrm{AO}}) \,|\, \mathrm{poc}$.

For a specific level of desynchronization, the values of m and n for each batch may be different. Therefore, the probability of a photon ending up in the channel for each batch depends on the outer cycle they are in and it will be different as provided in (3.23)

and Figures 3.7 and 3.8. We consider that for the batch with AO appearing in m' and n', $P_{\text{poc}_{m',n'}} = \left(1 - \lambda_{n',m'}\right)$. Therefore, from (3.28), the probability of Eve detection via photons intended for desynchronization estimation is

$$P_{S_{MN}}(|1\rangle_{\text{AO}}) = \frac{1}{(MN)^2}\frac{1}{(K+1)}\sum_{j=1}^{MN} j P_{\text{poc}_j}\left(\frac{K}{2MN}(1-2j) + \frac{1}{2}(2K+1)\right), \tag{3.28}$$

where $j = m' \times n'$.

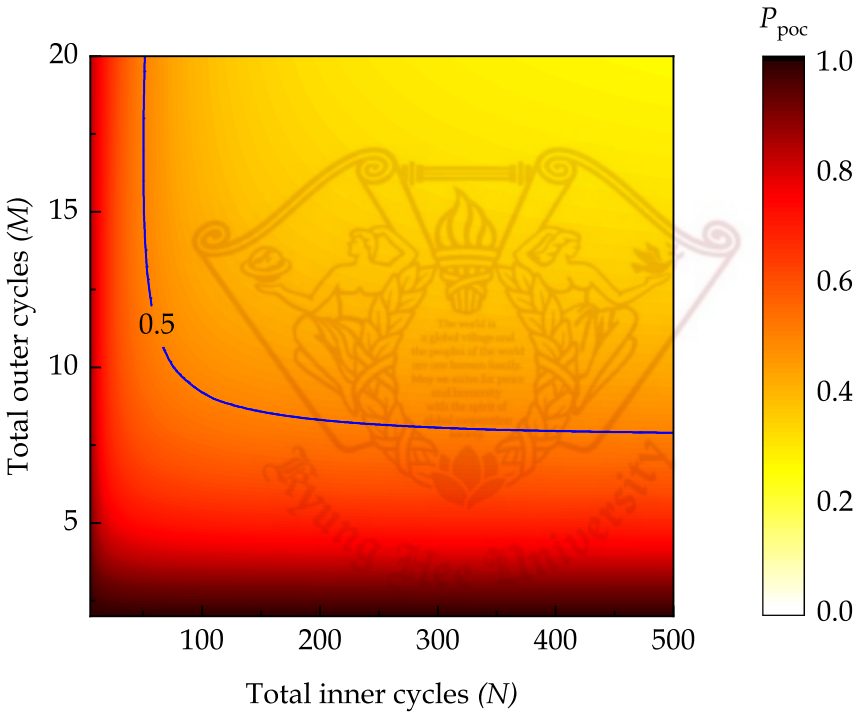


Figure 3.7: We plot the mean probability of a photon on the channel $\forall m, n$. As M and N increase, the probability decreases resulting in more photons for synchronization and lesser for Eve detection. At probability 0.5, we expect same number of photons for the two tasks.

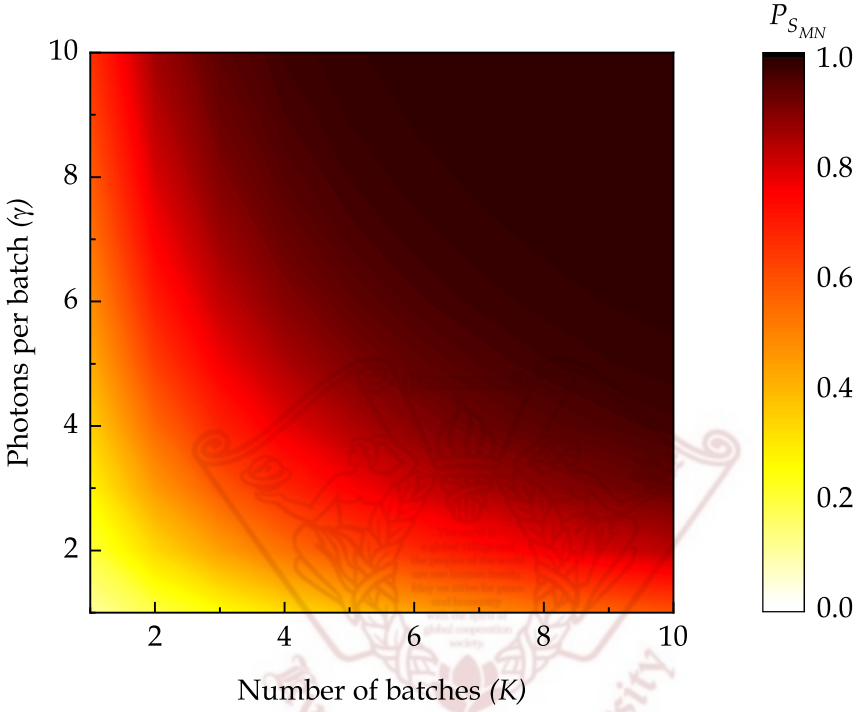


Figure 3.8: We set $M = 15$ and $N = 50$ corresponding to equal photons for synchronization and security and plot the probability of Eve detection (without using decay photons) $P_{S_{MN}}$ as a function of photon batches K and the number of photons each batch γ. $P_{S_{MN}}$ increases with an increase in both K and γ. The practical values of K and γ will depend on the experimental considerations including channel noise, required precision, and maximum desynchronization.

M	N							
	1	2	3	4	5	6	7	8
All Block	Eve cannot sabotage							
1	0	0	0	0	0	0	0	0
2	0.0019	0.0076	0.0076	0.0057	0.0096	0.0038	0.0076	0.0019
3	0	0.0019	0	0	0	0	0	0
All Pass	0.0287							

Table 3.1: For $\alpha \in \mathbb{W}$, $\phi_e \in [2\alpha\pi \pm 0.1, 2\alpha\pi \pm 2\pi \mp 0.1)$, expectation of undetectable sabotage $\left(|P_{\mathrm{e}}| < 4.0244 \times 10^{-4}\right)$ leading to error in desynchronization estimate.

3.2.4 Identification of relative frequency difference for channel delay attack

Considering limitations of the practical frequentist approach for identifying channel delay attack, the number of photons ℓ_d required to identify the difference between the relative frequencies of the two outcomes $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d} > |P_{\mathrm{e}}|_{\min} = 4.0244 \times 10^{-4}$ is very high. Therefore, we detect Eve if the $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d}$ is significantly higher, e.g., $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d} \geq 0.01$. For $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d} \geq 0.01$, the difference between the two relative frequencies is statistically significant with P value [94] < 0.05 for ℓ_d is of the order 5×10^4. leading to the detection of the adversary Eve. However, Eve is able to sabotage CSCS if the channel delay leads to $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d} < |P_{\mathrm{e}}|_{\min}$ *and* the ideal output state is not the nearest one to the practical output state. Table 3.1 and Table 3.2 provide the expectation of such cases for each of the possible outcomes for the minimum detectable $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d} > 4.0244 \times 10^{-4}$ and the practical case of $\left|\bar{P}_{\mathrm{e}}\right|_{\ell_d} > 0.01$, respectively.

M	N							
	1	2	3	4	5	6	7	8
All Block	Eve cannot sabotage							
1	0	0	0.0038	0.0019	0.0038	0.0038	0.0038	0
2	0.0076	0.0421	0.0593	0.0306	0.0516	0.0287	0.0325	0.0076
3	0.0115	0.0134	0.0115	0.0096	0.0019	0.0076	0.0115	0.0115
All Pass	0.0899							

Table 3.2: For $\alpha \in \mathbb{W}$, $\phi_e \in [2\alpha\pi \pm 0.1, 2\alpha\pi \pm 2\pi \mp 0.1)$, expectation of undetectable sabotage due to the limitation of frequentist approach limiting Eve detection and allowing Eve to sabotage without detection for $|P_{\mathrm{e}}| < 0.01$ leading to error in desynchronization estimate.

3.3 Discussion

In summary, we have provided a counterfactual scheme for clock synchronization, which is secure, precise, and robust against quantum channel noise. The key ingredient is a counterfactual conditional unitary which allows the client clock to identify and quantify the desynchronization. The CSCS scheme does not require any preshared phase reference between the server and client clocks. Unlike previous counterfactual schemes, we make use of the photons ending up in the channel alongside an authenticated public classical channel to provide security. Hence, the CSCS scheme does not require invoking an independent cryptography scheme for countering an adversary. The achieved precision of the scheme is inversely proportional to the quadratic power of the number of photon batches used, which is beyond the limit set on classical counterparts. This advantage is retained even in the presence of quantum noise in the channel. We envision that the CSCS scheme

would provide the synchronized operations for counterfactual communication and shared entanglement based protocols.

Chapter 4

Secure Counterfactual Byzantine Agreement

Quantum clock synchronization algorithms come under the broader umbrella of consensus algorithms for coordinated network tasks. These consensus algorithms constitute an agreement between distributed network nodes on a value or decision. They are at the core of cooperative networks and determine their performance to an extent [33]. Depending on a distributed network's specific nature and resources, its consensus algorithm can be tolerant against crash and/or malicious attack failure. The consensus algorithms that can tolerate malicious attacks are broadly classified under the umbrella of the BA [34]. Private correlated list distribution between network parties is the core task in BA for achieving this consensus.

For a tripartite network with one fault, BA is provably unsolvable [98, 99]. Nevertheless, a variant of BA called detectable BA circumvents this problem. It allows loyal parties to abort if they cannot agree on a decision [98]. In case of an abort, there may be a pre-decided strategy for the loyal parties depending on the scenario. It has been proven that classical resources alone cannot solve the detectable BA as well [99]. In recent

years, quantum correlations have been utilized for this task to achieve BA fault tolerance beyond the classical limit. Initially, QBA solutions were limited to three-party cases with a single faulty node. The first QBA protocol utilized Aharonov, N-particle N-level singlets to achieve private lists of six combinations [37, 38]. The same type of lists were shared using two quantum channels for key distribution [39]. Later, private lists with four possible correlated combinations were shared by employing four-qubit singlet states, QKD schemes, and Hardy correlations with entanglement swapping [40, 100, 101]. Through such quantum states, correlations, or QKD protocols, private random correlated lists are either shared between distributed processors, or the distribution is aborted. If the lists are successfully shared, they are used to achieve BA via classical authenticated channels. The entanglement-based protocols require an additional stage of verification that the entangled states have not been compromised [37, 102]. Furthermore, in QKD-based schemes and entangled states, the protocols require shared quantum phase reference to achieve QBA [102]. In recent years, quantum solutions for QBA focus on practically feasible agreements by avoiding the use of entanglement and QKD schemes. For these schemes, the agreement is achieved through the use of third-party semi-honest list distributors outside of the participants [103, 104]. However, as a trade-off, privacy is compromised due to the participation of semi-honest list distributors in the protocol of [104].

Recently, a private list distribution protocol has been proposed that utilizes a single un-entangled qudit [105, 106]. The qudit traverses to each node where the node encodes its information on the qudit and sends it to the next node. The unentangled nature of qudit and absence of any non-participants makes this protocol more scalable than entanglement-based schemes for practical consensus. On the flip side, as a consequence of such node traversing, the qudit and hence the private list becomes susceptible to external adversaries and Byzantine attacks by faulty nodes. Such attacks can sabotage the consensus procedure through man-in-the-middle attacks by either altering the list being shared or breaking the

secrecy of the shared list to use them for sabotaging the consensus stage e.g., for clock synchronization [58, 106].

In this chapter, we use the counterfactual communication paradigm for private list distribution based on the intuition behind qudit-based QBA. We focus on the problem of consensus in a network of up to one-half faulty nodes. The proposed protocol is not only secure against adversary attacks but does not lead to any information leakage to disloyal parties. The central node allows counterfactual computation to each node for achieving correlated lists without requiring the aid of any third party. Moreover, in contrast to existing quantum schemes, the proposed counterfactual BA (CBA) protocol does not require any shared phase reference between the distributed nodes [24, 107]. Finally, we demonstrate that security and privacy can be achieved for list distribution without any separate QKD scheme or requiring any *authenticated* or *secure* quantum channel.

The chapter is arranged as follows. In Section 4.1, we briefly overview the BA problem. Section 4.2 demonstrates the proposed protocol to distribute private lists in a K-partite network by means of counterfactual computation. We establish the privacy and security of the protocol against the quantum-equipped adversary in Section 4.3. We provide a conclusion and some possible future directions in Section 4.4.

4.1 Preliminaries

4.1.1 Byzantine Agreement

For a distributed network of n pairwise connected parties, BA is the method of achieving a coordinated behavior of the parties in the presence of faulty or dishonest nodes [98]. The coordinated behavior may be required for clock synchronization, secret sharing, or liar detection in a network [105,106]. In general, the fault may constitute a crash, omission, or Byzantine attacks at one or more nodes of the network. While the first two fault categories

constitute omission of all or a subset of messages, the Byzantine attack involves misleading information from the disloyal party to sabotage the coordination. The network has pair-wise authenticated error-free classical communication among the nodes. The network leader decides a value $x \in D$, from some finite domain D. The leader then communicates their choice to each party with the help of pair-wise communication channels. Then, the remaining nodes communicate pair-wise to mutually verify the message content. The network is said to have achieved BA if all nonfaulty nodes have verified and acknowledged the shared message x. Detectable BA is a relaxed version of BA which introduces the possibility of aborting the protocol in the absence of a consensus.

The BA protocol has been proven to be impossible to achieve unless each party has a private list suitably correlated with other parties in the network [34, 35]. Therefore, achieving BA essentially becomes the generation and distribution of private lists between network nodes [40]. A quantum protocol enables one to test the security of this list distribution. Thus quantum protocols are the best-suited candidates for list distribution. Such a quantum resource-based BA is often referred to as QBA. For quantum protocols, a protocol-specific quantum network is used for the list distribution stage in conjunction with the pairwise authenticated error-free classical channel network. In the next part, we explain the qudit-based QBA which will form the basis of our CBA [105].

4.1.2 Qudit-Based List Distribution

The detectable Byzantine agreement has previously been achieved through the use of quantum key distribution and entangled Aharnov states, singlet states, and GHZ-like states [37, 40, 102]. More recently, a qudit-based solution was proposed, which is more scalable than its entanglement-assisted counterparts [105, 106]. We review this protocol in the following.

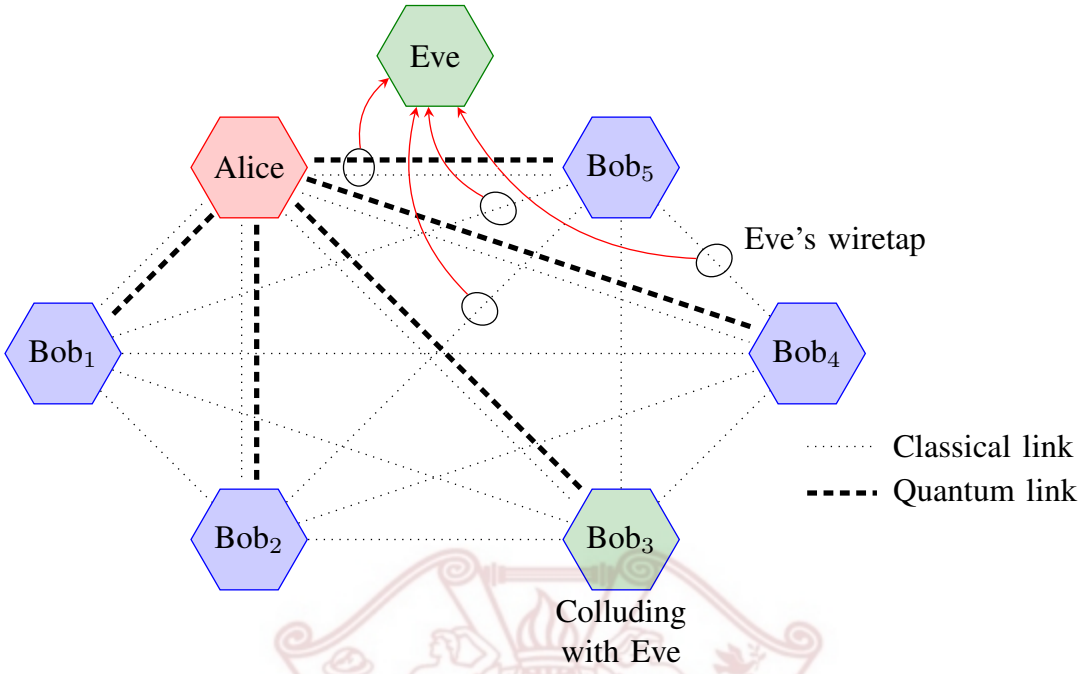


Figure 4.1: Network architecture for counterfactual secure BA. Alice shares a quantum channel with each of the Bob_i for the counterfactual private list distribution. Pairwise classical channels exist between all the nodes in the network for BA. An eavesdropper (Eve), either acting independently or under the direction of one of the malicious nodes (e.g., Bob_3) aims to sabotage the list distribution procedure.

4.2 Counterfactual List Distribution

The network consists of K nodes. The party (e.g., Alice), that wants to broadcast her message to the $K-1$ ordinary nodes (Bobs), becomes the central node. We denote the ith ordinary node as Bob_i. In the protocol, Alice prepares a K-dimensional qudit in the state

$$|\eta\rangle = \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |j\rangle \,, \tag{4.1}$$

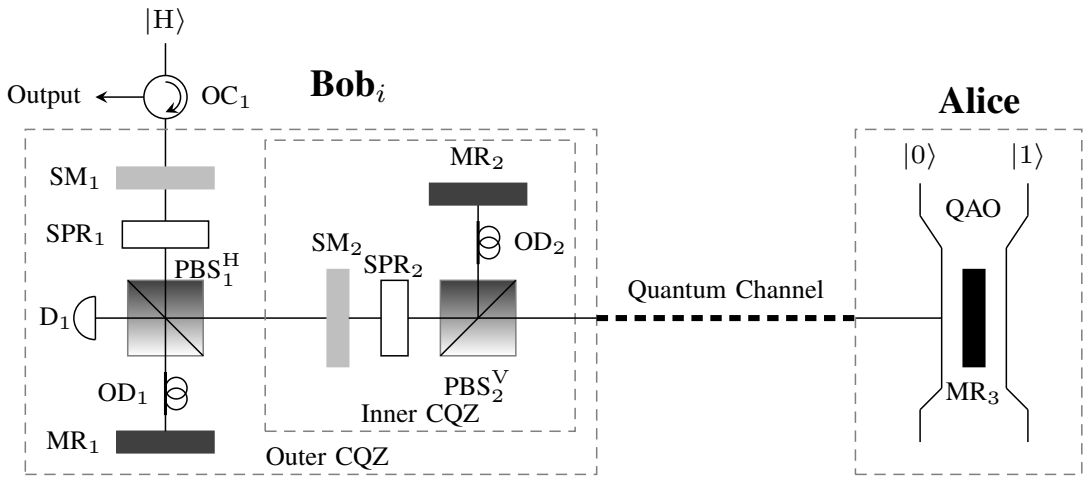


Figure 4.2: Setup for H-CQZ gate. It is composed of two cascaded CQZ gates. $|0\rangle$ ($|1\rangle$) represents the absence(presence) of QAO. On Alice's side, the optical elements are as follows: OC is an optical circulator, SM refers to a switchable mirror, SPR represents a switchable polarization rotator, PBS corresponds to a polarization beam splitter, and OD and MR are optical delay element and mirror respectively.

where $|j\rangle$ is the jth element of the standard (computational) basis. Alice applies the unitary operation $\boldsymbol{V}^{b_0}$ on the prepared qudit to encode her basis choice followed by $\boldsymbol{U}^{s_0}$ to encode secret entry, where

$$\boldsymbol{V} = |0\rangle\langle 0| + \sum_{k=1}^{K-1} \omega\, |k\rangle\langle k|\,, \tag{4.2}$$

$$\boldsymbol{U} = \sum_{\ell=0}^{K-1} \omega^{\ell}\, |\ell\rangle\langle \ell|\,, \tag{4.3}$$

with $\omega = e^{\frac{i2\pi}{K}}$, $b_0 \in \{0, 1, \cdots, K-1\}$ is her choice of basis encoding, and $s_0 \in \{0, 1, \cdots, K-1\}$ is her secret value for her private list.

Now, Alice sends the qudit to Bob_1, which applies $\boldsymbol{U}^{s_1}\boldsymbol{V}^{b_1}$ where $b_1 \in \{0, 1, \cdots, K-1\}$ and $s_1 \in \{0, 1\}$ are his choice of basis value, and the value for the secret list entry. Bob_1

forwards the qudit to Bob_2 and the procedure is continued until the qudit reaches Bob_{K-1} and he applies $\boldsymbol{U}^{s_{K-1}}\boldsymbol{V}^{b_{K-1}}$ according to his choice. Finally, Bob_{K-1} performs a projective measurement with the following projectors $\{|\eta\rangle\langle\eta|, I - |\eta\rangle\langle\eta|\}$. If the measurement outcome corresponding to $|\eta\rangle\langle\eta|$ is obtained, all Bobs reveal their basis choice b_i in the reverse order of qudit transmission. If $\sum_{i=0}^{K-1} b_i \mod K = 0$, the list distribution of values s_i is valid. The parties repeat the list distribution procedure to generate correlated private lists of length L. We denote by $\mathcal{L}_0$, the list held by Alice and by $\mathcal{L}_i$ the list held by Bob_i for $i \in \{1, \cdots, K-1\}$. Following the successful list distribution, the parties achieve BA with the aid of pair-wise classical communication as follows

1. Alice sends a message $\lambda_{0,i} \in \{0, 1\}$ to each Bob_i alongside the list of indices $x_{0,i}$ of all the entries of $\mathcal{L}_0$ that contain the message $\lambda_{0,i}$.

2. Bob_i verifies if $\lambda_{0,i}$ and $x_{0,i}$ correspond to entries in his own list and performs either of the following tasks:

   - If they match, he sends $\lambda_{i,j}$ and $x_{i,j}$ to each of the other Bob_j.
   - If $x_{0,i}$ is inconsistent with the corresponding entries in $\mathcal{L}_i$, Bob_i sends the symbol $\perp$ to other parties without any accompanying sublist, meaning he received inconsistent data.
   - In case of any other transmission from Bob_i, other nonfaulty participants identify it as faulty through BA.

   A nonfaulty Bob_i decides on $\lambda_{0,i}$ as his final decision unless messages from other Bobs persuade him to decide that Alice is faulty [106].

In this section, we develop a counterfactual computation-based protocol to securely distribute secret lists in a K-partite quantum network for BA without transmitting any physical particle over the quantum channel. We consider the same roles as before where

Alice acts as the central node and $K-1$ Bobs act as ordinary nodes. Figure 4.1 shows the network setup for our protocol. For simplicity, we assume $K = 2^k$ for some natural number k. In contrast to the qudit-based BA, the proposed protocol allows Alice to utilize a k-qubit system. Alice starts the protocol by preparing a k-qubit initial state

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{K}} \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \cdots \sum_{x_k=0}^{1} |x_1 x_2 \cdots x_k\rangle \\ &= \frac{1}{\sqrt{K}} \sum_{\vec{x}\in\{0,1\}^k} |\vec{x}\rangle \,. \end{aligned} \tag{4.4}$$

on k quantum absorptive objects (QAOs). Alice then locally applies $\boldsymbol{A} = \boldsymbol{U}^{s_0}\boldsymbol{V}^{b_0}$ on $|\psi\rangle$.

Next, Bob$_i$ will apply $\boldsymbol{B}_i = \boldsymbol{U}^{s_i}\boldsymbol{V}^{b_i}$ for $i = 1, 2, \cdots, K-1$. Bob utilizes H-CQZ gates as shown in figure 4.2 to ensure the counterfactuality of the proposed protocol where $b_i \in \{0, 1, ..., K-1\}$ and $s_i \in \{0, 1\}$. Consider that Bob$_i$ first applies $\boldsymbol{V}^{b_i}$, Alice and Bob$_i$ take the following steps to counterfactually implement $\boldsymbol{V}^{b_i}$ on the k-qubit system of Alice.

- Bob$_i$ starts by throwing his horizontal polarized photon $|\mathrm{H}\rangle$ towards the counterfactual remote unitary for $\boldsymbol{V}^{b_i}$ as illustrated in Figure 4.3a. The composite state of Alice and Bob$_i$ at this point is $|\eta_{0,i-1}\rangle = |\psi_{i-1}\rangle\,|\mathrm{H}\rangle$ where $|\psi_{i-1}\rangle$ is the state of QAOs held by Alice after Bob$_{i-1}$'s operation, i.e.,

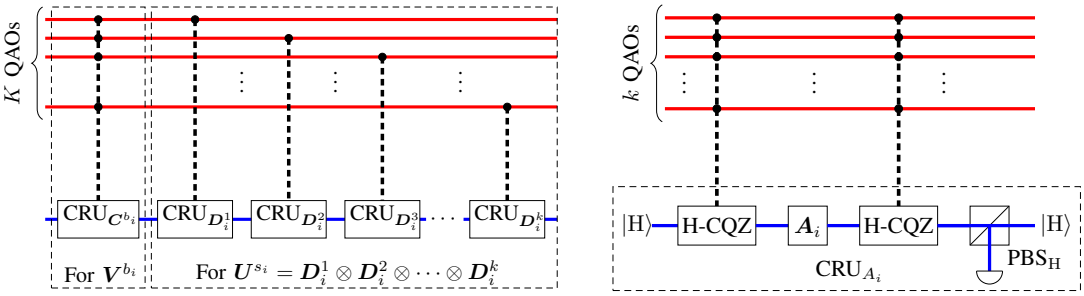
$$|\psi_{i-1}\rangle = \boldsymbol{B}_{i-1}\,|\psi_{i-2}\rangle\,, \tag{4.5}$$

  and $|\psi_0\rangle = \boldsymbol{A}\,|\psi\rangle$.

  Alice and Bob$_i$ apply $k+1$ qubits controlled unitary operation

$$\boldsymbol{Q} = |\vec{0}\rangle\langle\vec{0}| \otimes \boldsymbol{I} + \sum_{\substack{\vec{x}\in\{0,1\}^k \\ \vec{x}\neq\vec{0}}} |\vec{x}\rangle\langle\vec{x}| \otimes \sigma_x\sigma_z, \tag{4.6}$$

  on the composite state $|\eta_{0,i-1}\rangle$. Here σ_x and σ_z denote the Pauli-x and Pauli-z operators, respectively. For applying $\boldsymbol{Q}$, QAOs act as the control qubits and the



(a) (b)

Figure 4.3: Bob$_i$'s counterfactual encoding of her secret value and basis choice. (a) shows the complete counterfactual remote unitary (CRU) operation for each $\boldsymbol{V}^{b_i}$, and $\boldsymbol{D}_i^{\ell}$ and (b) shows the composition of each CRU gate. For $\boldsymbol{V}^{b_i}$ $k = K$ and $\boldsymbol{A}_i = \boldsymbol{C}_i$. While for each $\boldsymbol{D}_i^{\ell}$, $k = 1$ and $\boldsymbol{A}_i = \boldsymbol{D}_i^{\ell}$.

photon is the target qubit. Unless the photon is discarded in the H-CQZ gate, $\boldsymbol{Q}$ transforms the composite state $|\eta_{0,i-1}\rangle$ to

$$|\eta_{1,i-1}\rangle = \frac{1}{\sqrt{K}}\Big(|\vec{0}\rangle\,|\mathrm{H}\rangle + \sum_{\substack{\vec{x}\in\{0,1\}^k \\ \vec{x}\neq\vec{0}}} \alpha_{\vec{x}}^{(i-1)}\,|\vec{x}\rangle\,|\mathrm{V}\rangle\Big) \tag{4.7}$$

with probability [52, 76]

$$\lambda_1 = \big(1 - \frac{1}{K}\sin^2\theta_M\big)^M \prod_{m=1}^{M}\left[1 - \frac{K-1}{K}\sin^2(m\theta_M)\sin^2\theta_N\right]^N, \tag{4.8}$$

where $\alpha_{\vec{x}}^{(i-1)} = \omega^{js_{i-1}+b_{i-1}}\alpha_{\vec{x}}^{(i-2)}$, and j is the decimal representation of the binary vector $\vec{x}$.

- Bob$_i$ locally applies a single qubit unitary operation $\boldsymbol{C}_i = \boldsymbol{C}^{b_i}$, where

$$\boldsymbol{C} = \begin{pmatrix} 1 & 0 \\ 0 & -\omega \end{pmatrix}, \tag{4.9}$$

on his photon, which transforms the composite state $|\eta_{1,i-1}\rangle$ to

$$|\eta_{2,i-1}\rangle = \frac{1}{\sqrt{K}}\Big(|\vec{0}\rangle\,|\mathrm{H}\rangle - \sum_{\substack{\vec{x}\in\{0,1\}^k \\ \vec{x}\neq\vec{0}}} \omega^{b_i}\alpha_{\vec{x}}^{(i-1)}\,|\vec{x}\rangle\,|\mathrm{V}\rangle\Big). \tag{4.10}$$

Finally, Alice and Bob$_i$ again apply $\boldsymbol{Q}$ by using the H-CQZ gate (see Figure 4.3b) to complete the $\boldsymbol{V}^{b_i}$. Unless the photon is absorbed, it transforms the composite state $|\eta_{2,i-1}\rangle$ to

$$|\eta_{3,i-1}\rangle = \left(\boldsymbol{V}^{b_i}\otimes\boldsymbol{I}\right)|\psi_{i-1}\rangle\,|\mathrm{H}\rangle = |\phi_{0,i-1}\rangle\,|\mathrm{H}\rangle \tag{4.11}$$

with probability λ_1.

Since $\boldsymbol{U}^{s_i}$ is a separable unitary operation, it can be decomposed as

$$\boldsymbol{U}^{s_i} = \bigotimes_{\ell=1}^{k}\boldsymbol{D}_i^{\ell} \tag{4.12}$$

where $\boldsymbol{D}_i^{\ell} = \boldsymbol{C}^{\ell s_i}$ and ℓ denotes the ℓth qubit (QAO) held by Alice. In order to perform $\boldsymbol{D}_i^{\ell}$ on ℓth qubit, Alice and Bob$_i$ take the following steps.

1. Bob$_i$ throws his horizontal polarized photon $|\mathrm{H}\rangle$ towards the counterfactual remote unitary gate as illustrated in Figure 4.3a. Alice and Bob$_i$ apply 2 qubits controlled unitary operation $\tilde{\boldsymbol{Q}}_\ell$ on the composite state $|\tilde{\eta}_{0,i-1}\rangle = |\phi_{\ell-1,i-1}\rangle\,|\mathrm{H}\rangle$, where

$$|\phi_{\ell-1,i-1}\rangle = \left(\boldsymbol{I}^{\otimes(\ell-2)}\otimes\boldsymbol{D}_i^{\ell-1}\otimes\boldsymbol{I}^{\otimes(k-\ell+1)}\right)|\phi_{\ell-2,i-1}\rangle\,, \tag{4.13}$$

$$\tilde{\boldsymbol{Q}}_\ell = \sum_{\vec{x}\in\{0,1\}^k}|\vec{x}\rangle\langle\vec{x}|\otimes(\boldsymbol{XZ})^{x_\ell}\,. \tag{4.14}$$

Alice's ℓth QAO acts as the control qubit and Bob's photon is the target qubit. Unless the photon is discarded in the H-CQZ gate, $\tilde{\boldsymbol{Q}}_\ell$ transforms the composite

Protocol 4: Counterfactual $\boldsymbol{V}^{b_i}$ applied by Bob_i on Alice's QAOs.

Input: k: QAOs in the $|\psi_{i-1}\rangle$ state at Alice.

Input: Bob_i: ith receiver in list distribution, where $i \in \{1, \cdots, K-1\}$

Input: $|q\rangle_{\text{Bob}_i}$: photon in $|\text{H}\rangle$ state at Bob_i.

Input: $b_i \in \{0, 1, \cdots, K-1\}$: Bob_i's secret value.

Output: Obtain $|\phi_{0,i-1}\rangle = \boldsymbol{U}^{s_i} |\psi_{i-1}\rangle$

$|\eta_{0,i-1}\rangle \leftarrow |\phi_{\ell-1,i-1}\rangle |\text{H}\rangle$, ▶ Initial state of the photon & QAOs

$|\eta_{1,i-1}\rangle \leftarrow \boldsymbol{Q} |\eta_{0,i-1}\rangle$, ▶ Entangling operation

$|\eta_{2,i-1}\rangle \leftarrow \boldsymbol{I}^{\otimes k} \otimes \boldsymbol{C}^{b_i} |\eta_{1,i-1}\rangle$, ▶ Basis encoding

$|\eta_{3,i-1}\rangle \leftarrow \boldsymbol{Q} |\eta_{2,i-1}\rangle$, ▶ Disentangling operation

$|\psi_{i-1}\rangle |\text{H}\rangle \leftarrow |\eta_3\rangle$, ▶ Final state of the photon & QAOs

return $|\psi_i\rangle = |\phi_k, i-1\rangle$.

state $|\tilde{\eta}_{0,i-1}\rangle$ to

$$|\tilde{\eta}_{1,i-1}\rangle = \frac{1}{\sqrt{K}} \Big(\sum_{\substack{\vec{x} \backslash x_\ell \in \{0,1\}^{k-1} \\ x_{\ell=0}}} \beta_{\vec{x}}^{(\ell-1)} |\vec{x}\rangle |\text{H}\rangle + \sum_{\substack{\vec{x} \backslash x_\ell \in \{0,1\}^{k-1} \\ x_{\ell=1}}} \beta_{\vec{x}}^{(\ell-1)} |\vec{x}\rangle |\text{V}\rangle \Big) \tag{4.15}$$

with probability [52, 76]

$$\lambda_2 = \big(1 - \frac{1}{2} \sin^2 \theta_M\big)^M \prod_{m=1}^{M} \Big[1 - \frac{1}{2} \sin^2 (m\theta_M) \sin^2 \theta_N\Big]^N, \tag{4.16}$$

where $\beta_{\vec{x}}^{(\ell-1)} = \omega^{x_{\ell-1} s_i} \beta_{\vec{x}}^{(\ell-2)}$ and

$$\beta_{\vec{x}}^{(0)} = \begin{cases} 1, & \text{if } \vec{x} = \vec{0}, \\ \omega^{b_i} \alpha_{\vec{x}}^{(i-1)}, & \text{otherwise.} \end{cases} \tag{4.17}$$

Protocol 5: Counterfactual $\boldsymbol{U}^{s_i}$ applied by Bob_i on Alice's QAOs.

Input: k: QAOs in the $|\phi_{0,i-1}\rangle$ state at Alice.

Input: Bob_i: ith receiver in list distribution, where $i \in \{1, \cdots, K-1\}$

Input: $|q\rangle_{\text{Bob}_i}$: photon in $|\text{H}\rangle$ state at Bob_i.

Input: $s_i \in \{0, 1\}$: Bob_i's secret value.

Output: Obtain $|\psi_i\rangle = \boldsymbol{U}^{s_i} |\phi_{0,i-1}\rangle = \bigotimes_{\ell=1}^{k} \boldsymbol{D}_i^{\ell} |\phi_{0,i-1}\rangle$

for $\ell \in 1 \to k$ **do**

- $|\tilde{\eta}_{0,i-1}\rangle \leftarrow |\phi_{\ell-1,i-1}\rangle |\text{H}\rangle$, ▶ Initial state of the photon & QAOs
- $|\tilde{\eta}_{1,i-1}\rangle \leftarrow \tilde{\boldsymbol{Q}}_{\ell} |\tilde{\eta}_{0,i-1}\rangle$, ▶ Entangling operation
- $|\tilde{\eta}_{2,i-1}\rangle \leftarrow \boldsymbol{I}^{\otimes k} \otimes \boldsymbol{D}_i^{\ell} |\tilde{\eta}_{1,i-1}\rangle$, ▶ Basis encoding
- $|\tilde{\eta}_{3,i-1}\rangle \leftarrow \tilde{\boldsymbol{Q}}_{\ell} |\tilde{\eta}_{2,i-1}\rangle$, ▶ Disentangling operation
- $|\phi_{\ell,i-1}\rangle |\text{H}\rangle \leftarrow |\tilde{\eta}_{3,i-1}\rangle$, ▶ Final state of the photon & QAOs

return $|\psi_i\rangle = |\phi_k, i-1\rangle$.

2. Bob_i locally applies $\boldsymbol{D}_i^{\ell}$ on his qubit which transforms $|\tilde{\eta}_{1,i-1}\rangle$ to

$$|\tilde{\eta}_{2,i-1}\rangle = \frac{1}{\sqrt{K}} \Big(\sum_{\substack{\vec{x} \setminus x_\ell \in \{0,1\}^{k-1} \\ x_\ell = 0}} \beta_{\vec{x}}^{(\ell-1)} |\vec{x}\rangle |\text{H}\rangle - \sum_{\substack{\vec{x} \setminus x_\ell \in \{0,1\}^{k-1} \\ x_\ell = 1}} \omega^{\ell s_i} \beta_{\vec{x}}^{(\ell-1)} |\vec{x}\rangle |\text{V}\rangle \Big) \tag{4.18}$$

Alice and Bob_i again apply $\tilde{\boldsymbol{Q}}_{\ell}$ to disentangle the photon from the QAOs. Unless the photon is absorbed, it transforms the composite state $|\tilde{\eta}_{2,i-1}\rangle$ to

$$|\tilde{\eta}_{3,i-1}\rangle = \Big(\boldsymbol{D}_i^{\ell} \otimes \boldsymbol{I} \Big) |\phi_{\ell-1,i-1}\rangle |\text{H}\rangle = |\phi_{\ell,i-1}\rangle |\text{H}\rangle \,. \tag{4.19}$$

Alice and Bob_i repeat step 1 and 2 for $\ell \in \{1, 2, \cdots, k\}$ to complete the $\boldsymbol{U}^{s_i}$ operation. Note that $\alpha_{\vec{x}}^{(i)} = \beta_{\vec{x}}^{(k)}$ and $|\psi_i\rangle = \boldsymbol{U}^{s_i} |\phi_{0,i-1}\rangle$. Figure 4.3a shows the architecture for V^{b_i} and U^{s_i} operations counterfactually while Figure 4.3b shows the gates in each of them.

Once all nodes complete their operations, the central node measures the state of QAOs

Messages	Decision
$\forall j \in \mathcal{K}_i$, $x_{j,i} = x_{i,i}$ & $\lambda_{j,i} = \lambda_{i,i}$	$\lambda_{1,i}$, no faulty parties.
$\forall j \in \mathcal{K}_i$, $x_{j,i} = x_{i,i}$ & not all messages are equal	$\lambda_{j,i}$, if $> K/2$ parties (including Bob$_i$) hold $\lambda_{j,i}$, Abort, otherwise.
$\forall j \in \mathcal{M}_i \subset \mathcal{K}_i$, $x_{j,i} = x_{i,i}$ & $\forall j \notin \mathcal{M}_i \subset \mathcal{K}_i$, $x_{j,i} \neq x_{i,i}$	$\lambda_{j,i}, \forall j \in \mathcal{M}_i$, others are faulty.

Table 4.1: The decision of Bob$_i$ for the agreement stage of CBA. The second situation includes our modification to the original QBA [106].

in the Fourier basis $\{|\psi\rangle, |\psi^{\perp}\rangle\}$ [105]. Similar to the qudit-based protocols, if the measurement result is $|\psi\rangle$, all nodes reveal their choices of basis b_i. In contrast to the qudit-based BA, these bases are revealed in random order. The purpose of basis encoding and revealing is to prevent any party (especially the central node) from cheating in a way that leads to an invalid list distribution to be treated as valid. If $\sum_{i=0}^{K-1} b_i \mod K = 0$, the list distribution of values s_i is treated as valid. If Alice's entry in the list is $s_0 = 0(1)$, $s_i = 0(1) \forall i$. In case Alice's entry is $s_0 \in \{2, \cdots, K-1\}$, the corresponding anti-correlated list involves the sum of all Bobs' corresponding entries equal to $\sum_{s_i=1}^{K-1} s_i = K - s_0$.

The list distribution procedure is repeated to generate correlated private lists of length L. Following the successful list distribution, the parties achieve BA by exchanging classical messages as mentioned in the Section 4.1. Table 1 shows the decisions taken by Bob$_i$ given the set of messages and indices $\mathcal{K}_i = \{\{\lambda_{0,i}, x_{0,i}\}, \{\lambda_{1,i}, x_{1,i}\}, \cdots, \{\lambda_{K-1,i}, x_{K-1,i}\}\}$ that he receives from all the other parties. He compares the received indices with the corresponding entries in his list $\mathcal{L}_i$. The BA procedure for qudit-based BA suffers from indecision in the event of $\perp$ messages and faulty P_1 [106,108]. To avoid such indecision, we modify the BA procedure [106] as follows: First, Bob$_i$ ignores all the $\perp$ messages (although

the existence of $\perp$ indicates that Alice is maybe faulty). Now, if the sublists are all same but messages are different, then choose the message sent by at least $K/2$ parties. If none of the messages appears with $K/2$ frequency, Bob_i must choose abort.

One crucial advantage of our CBA protocol is that it does not require any shared phase reference between the network nodes [32,107]. Since Alice and Bob_i hold their own qubits and the only action between Alice's QAO and Bob_i's photon is the absorption of channel components; therefore, the local choice of phase reference can be independent [107]. In the previous implementations of QBA, quantum systems are prepared by one party and they travel to other parties where they undergo quantum evolution/measurement [37, 38, 40, 101–106]. Therefore, for these schemes, shared phase reference is a necessary requirement [32,107]. For our CBA, this removes the requirement of a prior quantum handshake of the network nodes. However, as a trade-off, the success probability of H-CQZ implementation is not 1. Figures 4.4 and 4.5 show the successful implementation of H-CQZ gates for V^{b_i} and D_i^{ℓ} respectively.

4.3 Security of Counterfactual Byzantine Agreement

In the presence of pairwise authenticated classical channels, the security of the Byzantine agreement boils down to the security of the distributed lists [40]. A malicious agent might attack the list distribution protocol to either sabotage it or steal some information about the list being shared. Sabotage may result in the distribution of incorrect list entries or may cause some form of denial-of-service attack. In the following, we consider different possible attacks in the list distribution protocol and discuss protection against these attacks.

4.3.1 Intercept-and-Resend Attack

First we consider the case of an intercept and resend attack by a non-participant Eve. In this attack, Eve intercepts the qubit in the channel traveling from one legitimate user

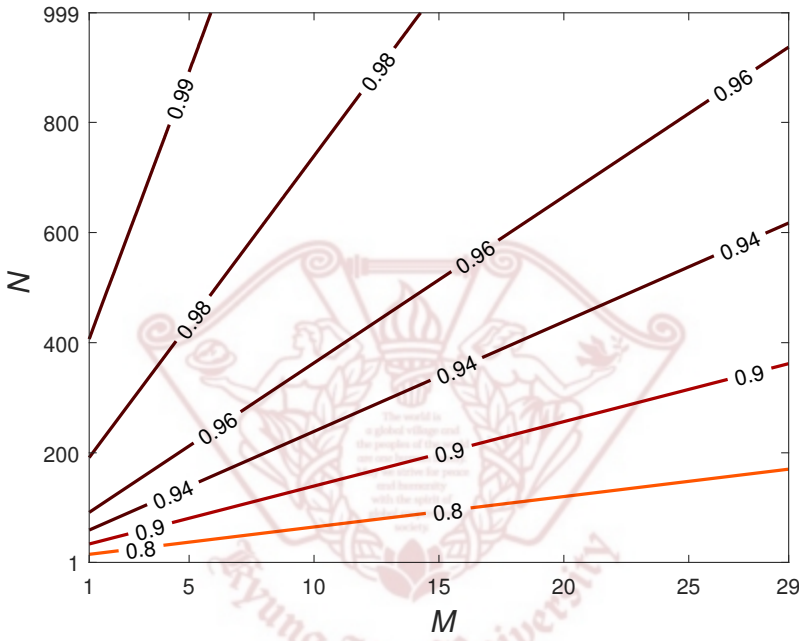


Figure 4.4: Success probability λ_1 as functions of M and N. We plot the success probabilities of an H-CQZ gate for V^{b_i} as functions of the number of outer cycles M and the number of inner cycles N in a network of $K = 8$ nodes.

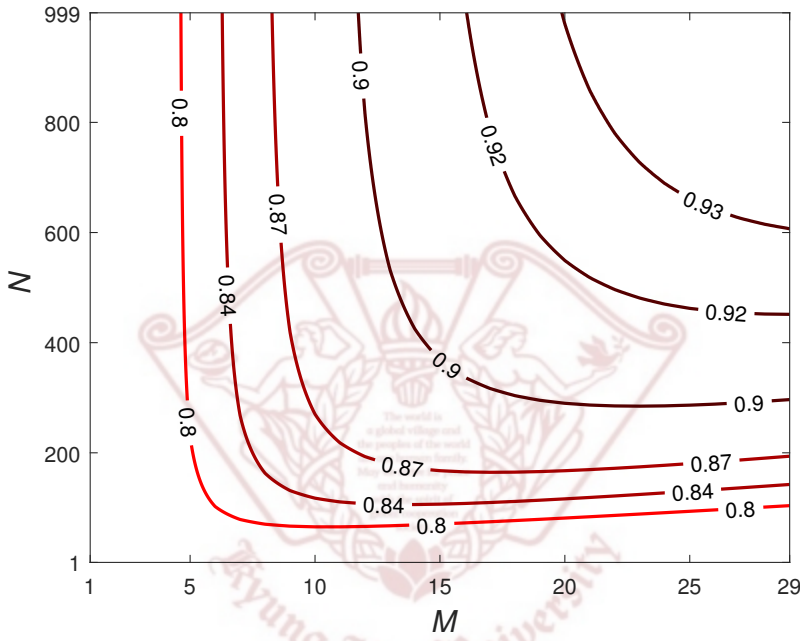


Figure 4.5: Success probability λ_2 as functions of M and N. We plot the success probabilities of an H-CQZ gate for D_i^ℓ as functions of the number of outer cycles M and the number of inner cycles N in a network of $K = 8$ nodes.

to another. She can measure the qubit immediately followed by preparing a new qubit based on the measurement result. Alternatively, she can store the intercepted qubit in her quantum memory and send a new qubit to the receiver.

The proposed CBA protocol is secure against this class of attacks because of the counterfactual nature of the CBA. In a counterfactual setup, no information-carrying particle appears on any channel accessible to Eve. In case of any particle appears on the channel, that round of communication is discarded to keep the protocol counterfactual. This eliminates the possibility of intercepting any information carrying qubit. Furthermore, Eve only has access to the $|\mathrm{H}\rangle$ component of the photon wavefunction that enters the channel in each cycle. Hence, the entropy over the channel is 0. Therefore, Eve's interception of $|\mathrm{H}\rangle$ does not give her any new information.

If Eve's purpose is to sabotage the list distribution, she can block and or reflect the photon wave-function randomly. To counter this denial-of-service attack, Bob_i either uses decoy photons sent directly into the channel or counterfactually used photons ending up in the channel. If Bob_i sends decoy photons in the channel, it stops the list distribution procedure to detect Eve. The probability with which Bob_i may use a decoy photon is a function of M, N, and the required success probability of Eve's detection. If the photon in the channel interacts with Alice's QAO it gets absorbed. If the photon does not interact with Alice's QAO, it is reflected back to Bob and is absorbed before the start of the new outer cycle. For $\boldsymbol{V}^{b_i}$ gate, Bob_i's photon has $(K-1)/K$ probability that at least one QAO exists in its path. While for each $\boldsymbol{D}_i^{\ell}$ for $\boldsymbol{U}^{s_i}$ gate, Bob_i's photon has $1/2$ probability that the corresponding QAO is in its path. Therefore, based on M and N, if the actual detection frequency is different from Alice's detection probability, the presence of Eve is indicated.

4.3.2 Man in the Middle Attack

For general consensus schemes like correlated list distribution, another significant attack is the MITM attack where Eve impersonates a legitimate party. For our counterfactual setup, this means Eve acting either as Alice or as Bob_i or as both.

1. **As Alice:** Eve may try to impersonate Alice by blocking the channel through her own QAOs. This scenario is similar to the intercept attack, which can be countered by Bob using decoy photons and particles in the channel to identify the presence of Eve.

2. **As Bob_i:** Eve may try to impersonate Bob by applying her own $\boldsymbol{U}\,(\boldsymbol{V})$ through her own auxiliary photons. If Eve does not use a counterfactual setup, she will not be able to make this attack since Alice can ascertain Eve's presence confirming the absorbed photon did not belong to Bob_i.

   In case Eve utilizes a counterfactual H-CQZ gate to apply $\boldsymbol{U}\,(\boldsymbol{V})$, Eve's detection is possible through the photons that end up in the channel as follows. We consider near perfect detectors at Alice with the detection range $\{f_{\min}, f_{\min} + \Delta f, f_{\min} + 2\Delta f, \cdots, f_{\min} + n\Delta f\}$. Bob can uniformly choose a random frequency f_{Bob_i} from this range for his $|\text{H}\rangle$ polarized photon. The probability that his frequency is different from the randomly chosen frequency of Eve's auxiliary photon is $1 - \frac{1}{n}$. This use of random frequency allows a frequency signature for Bob_i which becomes relevant whenever Alice detects a photon. For previous quantum schemes for list distribution, there was no signature for quantum information transfer. This use of frequency signature for quantum information transfer (in the absence of authenticated quantum channels) makes our implementation of BA comparable to classical schemes with authenticated classical channels for the entire BA. Eve's setup being counterfactual will lead to her photon ending up in the channel with some probability. Therefore,

if a photon is absorbed at Alice, Eve can be detected by classical communication about the Bob_i's photon's frequency. In comparison, Eve has total access of Alice's qudit for qudit-based BA protocol, thereby allowing it to infer the qudit state [62].

Furthermore, previous schemes have no way of identifying Eve through her signature. The only way to detect Eve's presence in their case is to reveal a part of the list and see if the quantum error rate (QER) is beyond a threshold [40,105,109]. Furthermore, if Eve leads to an unchecked correct list, the QBA can fail [105]. This is a problem since previous quantum schemes claim either abort of correct QBA alone.

4.3.3 Trojan Horse Attack

Trojan horse attack involves the use of auxiliary photons by Eve to gain information about the apparatus of legitimate parties by analyzing this reflected photon [110].

1. **Targeting Bob's end:** On Bob's end, a fixed H-CQZ unit is attached to the channel. Eve cannot gain any information using her probing photon, since the setup is publicly known and fixed. The changing components belong to the local computation unit performing the gate $\boldsymbol{D}_i^{\ell}$ or $\boldsymbol{C}_i$. But the local computational elements are inaccessible to Eve's photon.

2. **Targeting Alice's end:** On Alice's end, the state of the QAO system is evolving under the action of $\boldsymbol{U}$ and $\boldsymbol{V}$ from each party. Alice's QAOs are individually accessible to Eve during the $\boldsymbol{U}$ operation by Bob. Conventionally, Eve can use a photon of either a different wavelength or in a different time window and send it to Alice directly. But with near-perfect detectors, this attack fails because Alice's absorption of Eve's photon can be communicated between legitimate parties to establish the presence of Eve [110].

   A counterfactual Trojan horse attack is another possibility, wherein, Eve sends a polarized photonic component into the channel towards Alice. However, due to its

counterfactual nature, the photon may enter the channel resulting in Eve's detection. In case it is undetected, only the channel component of the photon repetitively interacts with QAO and is either reflected or absorbed. This does not give her enough information to perfectly distinguish between the different possible states of QAO [62, 111].

4.3.4 Entangle and Measure Attack

Eve can entangle her photons with Alice, and measure them to project Alice's QAOs into some state. Eve can do this for both $\boldsymbol{U}$ $(\boldsymbol{V})$ gates. However, this entangle and measure attack will lead the final state to a non-Fourier basis state [105]. If Eve is suspected of launching this attack, the protocol may be run multiple times with the same configuration (choice commitment from all parties) [105]. Measuring multiple copies with the same configuration should result in the same measurement outcome in the absence of Eve. Hence, Eve's presence will be detected in case of different measurement outcomes for multiple runs. This is unlike the case of previous protocols [105] wherein Eve had full access to the qudit and could use Fourier basis measurement herself.

4.4 Conclusion

In this work, we have utilized the counterfactual computation to securely distribute correlated private lists for Byzantine agreements. Our protocol works in the absence of shared phase reference, which is a key necessity for previous quantum schemes for list distribution. We show that our scheme is secure against an external adversary or a colluding party with malicious intent. This makes our scheme a suitable candidate for secure clock synchronization and permissioned enterprise-level small-scale consortium blockchains like modular computing units [33, 106].

Future works may include integrating CBA with a consortium blockchain like Zilliqa

and Hyperledger fabric [33] and its testing in a consortium blockchain network. Furthermore, the comparison and/or integration of CBA with the widely used Practical Byzantine Fault Tolerant can be considered for the future versions of Hyperledger Fabric and Zilliqa blockchains.

Chapter 5

Noise-Robust Counterfactual Consensus

As discussed in previous chapters, counterfactual communication-based schemes provide an unprecedented advantage for distributed quantum networks. In this chapter, we will investigate the practicality of these schemes in the NISQ era networks. We first introduce entanglement distribution before providing a counterfactual noise-robust version of this for counterfactual consensus to highlight the practicality of chained quantum Zeno gates for NISQ networks.

Recently, DCC has been experimentally implemented through a single-photon source to transfer a monochrome bitmap from one location to another [65]. The noise analysis of a single-photon-based DCC has been limited to path scattering and detector, and optical element inefficiencies [52, 70].

Shared prior entanglement is at the heart of a range of quantum protocols [57, 112]. However, the fidelity of the preshared entanglement relies on the common phase reference between Alice and Bob [32, 107]. In practice, this requirement of sharing nonfungible information is hard to achieve [107].

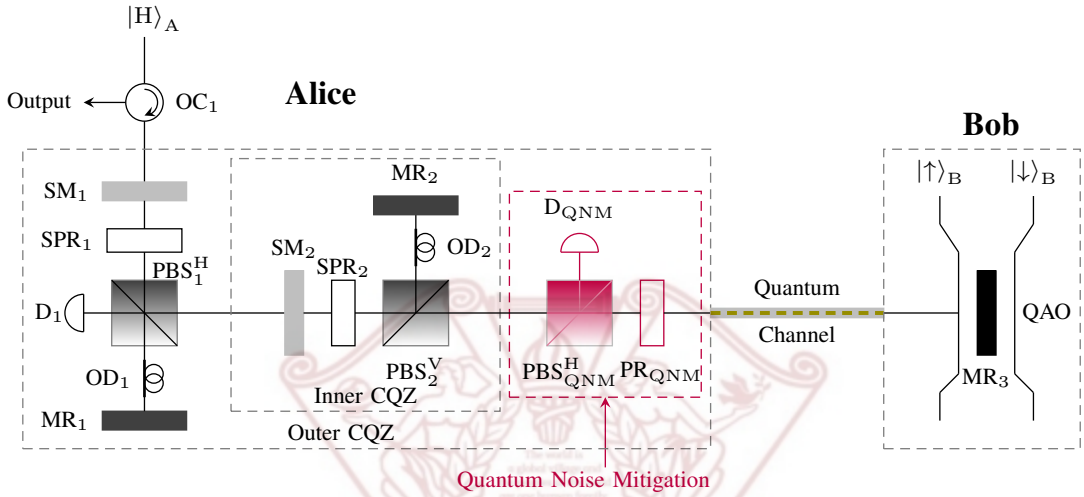


Figure 5.1: Schematic for H-CQZ$_{QNM}$ gate for quantum entanglement distribution. It is made up of two cascaded CQZ gates at Alice's end. The optical elements are as follows: OC is an optical circulator, SM refers to a switchable mirror, SPR represents a switchable polarization rotator, PBS corresponds to a polarization beam splitter, and OD and MR are optical delay elements and mirror respectively. Here, PBS_1^H (PBS_2^V) reflects V(H) component and transmits H(V) component. On Bob's end $|\uparrow\rangle_B$ ($|\downarrow\rangle_B$) represents the presence(absence) of QAO.

In this chapter, we investigate the noise-robustness of the counterfactual consensus scheme, based on the DCC, that does not require any shared phase reference. Specifically, we consider the noise in the entangling H-CQZ gate. To make our scheme robust against noise, we modify the original DCC by introducing a quantum noise mitigation setup as shown in Figure 5.1. We then investigate the proposed scheme for the noise suffered by the remotely controlled properties (path and polarization) in the counterfactual interferometric system. We analyze the performance of our scheme in the presence of phase diffusion, interferometric invisibility, and photonic dispersion losses affecting the path DOF alongside the polarization DOF noise models, including dephasing, bit-flip, and depolarizing noise. We show that our counterfactual entangling operation in counterfactual consensus is robust against channel delay and dephasing noise all the while outperforming the conventional entanglement distribution for the remaining noise models as well.

The chapter is arranged as follows. In Section 5.1, we first introduce the modified DCC setup. Then, we provide the setup for counterfactual entanglement distribution used in the consensus scheme. We establish the robustness of our modified DCC-based counterfactual entanglement distribution against the absence of shared phase reference and quantum noise in Section 5.2. Finally, we provide a conclusion and future directions in Section 5.3.

5.1 Modified Direct Counterfactual Communication (DCC)

Taking account of the combined logic of interaction-free measurement (IFM) and the CQZ effect, counterfactual communication enables the direct transmission of information between two communicators (say Alice and Bob) in a particle-less manner. In this section, we first review the original DCC setup before providing the modified DCC setup for noise-robust counterfactual entanglement distribution.

5.1.1 Direct Counterfactual Communication Setup

The practical setup of DCC is realized through two cascaded Michelson interferometers as shown in Figure 5.1. Alice inputs a horizontally polarized photon ($|\mathrm{H}\rangle_{\mathrm{A}}$) into her H-CQZ gate located at one end of the quantum transmission channel and Bob counterfactually controls the polarization of the photon through an absorptive object. The absorptive object either blocks or unblocks the photonic wave function in the channel. The blocking and unblocking action by Bob controls the photon polarization state even though the photon never visited Bob. For logical 1, Bob blocks, leading to a $|\mathrm{H}\rangle_{\mathrm{A}} \rightarrow |\mathrm{V}\rangle_{\mathrm{A}}$ rotation on the photon. For logical 0, Bob does not block, which leaves the photon state unchanged. $|\uparrow\rangle_{\mathrm{B}}$ ($|\downarrow\rangle_{\mathrm{B}}$) represents the block (unblock) state of AO.

Alice performs M cycles of the outer interferometer. Inside each outer cycle, She performs N cycles of the inner Michelson interferometer. The value of $M\,(N)$ is decided by the success probability of the counterfactual setup as discussed later in Section 5.2.4. Alice starts the H-CQZ operation by inputting the $|\mathrm{H}\rangle_{\mathrm{A}}$-polarized photon into the outer interferometer. The photon encounters SPR_1 that rotates its polarization. In general, SPR rotates the photon polarization as

$$|\mathrm{H}\rangle_{\mathrm{A}} \rightarrow \cos\theta_K\,|\mathrm{H}\rangle_{\mathrm{A}} + \sin\theta_K\,|\mathrm{V}\rangle_{\mathrm{A}}\,, \tag{5.1}$$

$$|\mathrm{V}\rangle_{\mathrm{A}} \rightarrow \cos\theta_K\,|\mathrm{V}\rangle_{\mathrm{A}} - \sin\theta_K\,|\mathrm{H}\rangle_{\mathrm{A}}\,. \tag{5.2}$$

where $\theta_K = \frac{\pi}{2K}$ and $K = M\,(N)$ is an integer. For our setup, the SPR_1 rotates the input state $|\mathrm{H}\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{path}}$ to $\alpha\,|\mathrm{H}\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{path}} + \beta\,|\mathrm{V}\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{path}}$. Then the $\mathrm{PBS}_1^{\mathrm{H}}$ divides the photonic wave-function into two paths depending on the polarization state. The H-polarized component will stay in the same path $|0\rangle_{\mathrm{path}}$, while the V-polarized component enters into the

inner interferometer via $|1\rangle_{\text{path}}$. The PBS_1^{H} acts as

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha\,|\text{H}\rangle_{\text{A}}\,|0\rangle_{\text{path}} \\ 0 \\ \beta\,|\text{V}\rangle_{\text{A}}\,|0\rangle_{\text{path}} \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha\,|\text{H}\rangle_{\text{A}}\,|0\rangle_{\text{path}} \\ 0 \\ 0 \\ \beta\,|\text{V}\rangle_{\text{A}}\,|1\rangle_{\text{path}} \end{bmatrix}. \tag{5.3}$$

The V-polarized component in $|1\rangle_{\text{path}}$ encounters SPR_2 followed by the PBS_2^{V} which makes the H-component in $|1\rangle_{\text{path}}$ to enter channel via $|2\rangle_{\text{path}}$. If Bob's AO is present i.e., in the $|\uparrow\rangle_{\text{B}}$ state, it blocks the photonic wave-component in the channel collapsing the wave-function. However, if AO is absent i.e., in the $|\downarrow\rangle_{\text{B}}$ state, the mirror M_3 reflects the wave-component. After this, the reflecting component interferes with V-component in $|1\rangle_{\text{path}}$ at PBS_2^{V}. After interference, the photonic wave function in the inner interferometer loops back to start the next inner cycle. The state of the photon after the n^{th} cycle for the unblocking case is

$$|\text{H}\rangle_{\text{A}} \rightarrow \cos n\theta_N\,|\text{H}\rangle_{\text{A}} + \sin n\theta_N\,|\text{V}\rangle_{\text{A}} \xrightarrow{n=N} |\text{V}\rangle_{\text{A}}\,, \tag{5.4}$$

while for the blocking case, the state is

$$|\text{H}\rangle_{\text{A}} \rightarrow \cos^{n-1}(\cos\theta_N\,|\text{H}\rangle_{\text{A}} + \sin\theta_N\,|\text{V}\rangle_{\text{A}}) \xrightarrow{n=N} |\text{H}\rangle_{\text{A}}\,. \tag{5.5}$$

After the completion of N inner cycles, the polarization components form $|0\rangle_{\text{path}}$ and $|1\rangle_{\text{path}}$ interfere at PBS_1^{H}. D_3 absorbs any $|\text{V}\rangle_{\text{A}}$ component that comes out of the inner interferometer. This completes one outer cycle and the photon loops back to start the next outer cycle. In order to achieve counterfactual communication, Alice completes M times of the outer interferometer. The state of the photon for the unblocking case after the m^{th} cycle is

$$|\text{H}\rangle_{\text{A}} \rightarrow \cos^{m-1}(\cos\theta_M\,|\text{H}\rangle_{\text{A}} + \sin\theta_M\,|\text{V}\rangle_{\text{A}}) \xrightarrow{n=M} |\text{H}\rangle_{\text{A}}\,, \tag{5.6}$$

while for the blocking case, the state is

$$|\mathrm{H}\rangle_{\mathrm{A}} \rightarrow \cos n\theta_M |\mathrm{H}\rangle_{\mathrm{A}} + \sin n\theta_M |\mathrm{V}\rangle_{\mathrm{A}} \xrightarrow{n=M} |\mathrm{V}\rangle_{\mathrm{A}} . \tag{5.7}$$

It can be seen clearly that as the number of inner and outer cycles (N and M) approaches infinity, the chance of an information-carrying particle passing through the channel approaches zero. As a result, a classical bit can be transmitted counterfactually depending on Bob's action of blocking or unblocking the polarization property of the photon [60].

NOISE-ROBUST COUNTERFACTUAL ENTANGLEMENT DISTRIBUTION

Recently, some counterfactual entanglement distribution mechanisms have been proposed based on the DCC protocol [63, 70, 74]. These utilize a quantum AO (QAO) which can exist in a superposition of the blocking ($|\uparrow\rangle_{\mathrm{B}}$) and unblocking ($|\downarrow\rangle_{\mathrm{B}}$) states.

Consider that Bob holds a QAO in the maximal superposition state $\frac{1}{\sqrt{2}}(|\uparrow\rangle_{\mathrm{B}} + |\downarrow\rangle_{\mathrm{B}})$. Initially, the joint state of Alice's photon and Bob's QAO is

$$|\psi\rangle_1 = |\mathrm{H}\rangle_{\mathrm{A}} \otimes \frac{1}{\sqrt{2}}(|\uparrow\rangle_{\mathrm{B}} + |\downarrow\rangle_{\mathrm{B}}). \tag{5.8}$$

As discussed before, if Bob's QAO is in state $|\uparrow\rangle_{\mathrm{B}}$, it rotates the polarization of Alice's photon from H to V after the complete H-CQZ operation. On the other hand, the polarization of Alice's photon remains unchanged if Bob decides to put QAO in the $|\downarrow\rangle_{\mathrm{B}}$ state. Hence, the combined action of blocking and unblocking by Bob leads to

$$|\psi\rangle_1 \rightarrow |\psi\rangle_2 = \frac{1}{\sqrt{2}} \left(|\mathrm{H}\rangle_{\mathrm{A}} |\downarrow\rangle_{\mathrm{B}} + |\mathrm{V}\rangle_{\mathrm{A}} |\uparrow\rangle_{\mathrm{B}}\right). \tag{5.9}$$

Therefore, the entanglement has been shared between Alice and Bob, but no information-carrying particle passes through the channel.

We modify the DCC setup to make it noise-robust and develop a counterfactual entanglement distribution system. To account for the quantum channel noise, we modify the DCC through a quantum noise mitigation setup as highlighted in the Figure 5.1. It is

to be noted here that this modification becomes a necessity for polarization DOF noise on the channel component of the photon [65, 113]. We employ $\text{PBS}^{\text{H}}_{\text{QNM}}$ with detector D_{QNM} to remove any V-component that appears due to polarization DOF noise. The purpose of PR_{QNM} is to transform the $|\text{H}\rangle$ component in $|2\rangle_{\text{path}}$ to a suitable polarization given channel state information. The detailed utilization of noise mitigation setup has been provided in the next section.

To initiate the protocol, Alice inputs her first H-polarized photon into the first H-CQZ_{QNM} gate while Bob holds QAO in a maximal superposition state. At the output of the first H-CQZ_{QNM}, an EPR pair is created between Bob's QAO and Alice's photon according to (5.9).

5.2 Protection of counterfactual system against Noise

Quantum noise has been the fundamental bottleneck in the implementation of practical quantum computation and communication systems. In this section, we investigate the performance of counterfactual quantum information transfer against both unspeakable and speakable quantum noise [107]. The unspeakable quantum noise refers to the absence of shared phase reference between the distributed parties. While speakable quantum noise constitutes channel and local quantum noise affecting the involved DOFs of a quantum system. For the counterfactual system, these are path and polarization DOFs of a photon on Alice's end and QAOs at Bob's end. For the counterfactual interferometric setup, Salih et al. discussed the detector and optical element inefficiency in their analysis of the DCC for classical communication [52]. Later, a counterfactual-like communication based on coherent light was analyzed by [114, 115]. However, this analysis is limited to the interferometric noise affecting multi-photon non-polarization states unlike the single-photon polarization state utilized in DCC [52, 65]. The single-photon implementation almost inhibits phase diffusion via active phase stabilization to obtain a near-perfect result

[65]. For the active phase stabilization, two Piezoceramic translation stages are utilized. So far, there has been no noise analysis of the DCC encompassing the polarization and path analysis which as we shall see in the next subsection requires modifications to the original DCC-based information transfer schemes. We now perform this analysis for counterfactual entanglement distribution and show how these modifications make DCC-based schemes robust compared to direct quantum communication-based schemes.

5.2.1 Absence of Shared Phase Reference

Pre-shared entanglement (especially singlets $|\phi^-\rangle$) between Alice and Bob is a necessary ingredient for some of the groundbreaking quantum protocols. These include teleportation, entanglement-assisted quantum key distribution, and the revolutionary quantum clock synchronization protocol that does not require any real-time communication [29, 32, 112, 116, 117]. Conventionally, entanglement sharing is a prepare-and-share approach in which one party (say Alice) prepares X entangled states locally and then shares one particle of each entangled state with Bob [24, 29, 32]. However, this method of entanglement sharing is prone to *quantum* infidelity in the absence of the shared phase reference between Alice and Bob [107]. This is because the shared entanglement is in Alice's basis definition and not the local basis definition of each party, i.e., [32]

$$\frac{1}{\sqrt{2}}\left(|10\rangle_{\mathrm{A}} - |01\rangle_{\mathrm{A}}\right) \not\equiv \frac{1}{\sqrt{2}}\left(|1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} - |0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}\right). \tag{5.10}$$

Recently, entanglement purification has been identified as a possible solution to counter the absence of shared phase reference [32,57]. In this procedure, using the quantum circuit method, Bennet *et al.*'s entanglement purification is iteratively used to obtain singlets in the local basis [57]. However, it leads to the loss of half population of entangled states in each purification cycle. Furthermore, the fidelity F_n of the entangled pairs after n rounds

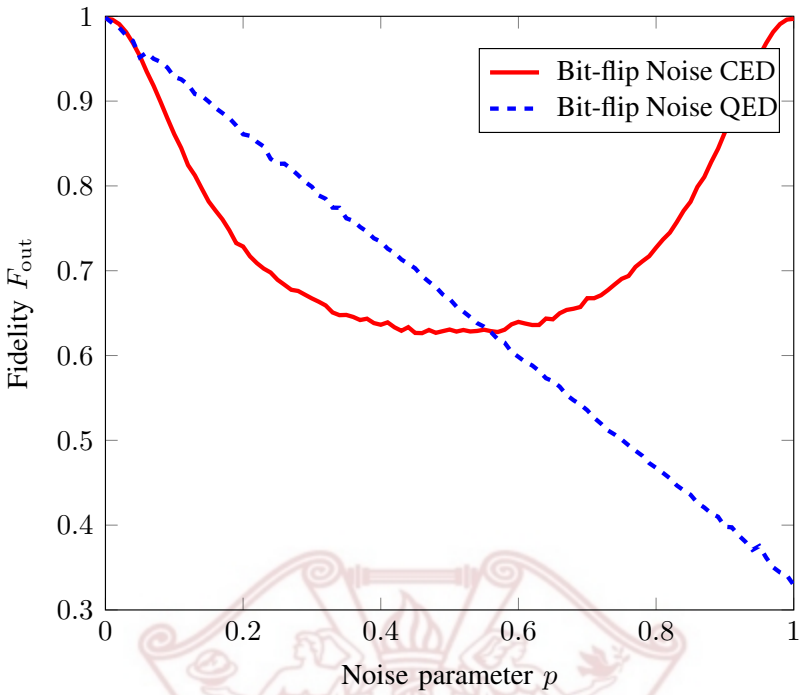


Figure 5.2: Fidelity of the distributed entangled state for bit-flip noise.

of purification is [57]

$$F_n = \frac{F_{n-1}^2 + \frac{1}{9}(1-F_{n-1})^2}{F_{n-1}^2 + \frac{2}{3}F_{n-1}(1-F_{n-1}) + \frac{5}{9}(1-F_{n-1})^2}, \tag{5.11}$$

where F_{n-1} is the fidelity after $(n-1)$th round of purification. After the nth round, the X entangled states are *reduced* to $X/2^n$ singlets. Furthermore, the probability of discarding the results of purification for a round is *non-zero*.

For counterfactual communication, the quantum operations on a qubit are always local. The QAO does not evolve during the operation. Meanwhile, the H-polarized photon undergoes quantum transformations at Alice's end only. The only action from Bob's QAO and AO on the photon is either reflection or absorption of the H-component on the channel. Therefore, our setup allows independent local definitions of phase reference. This makes our setup practical for plug-and-play networks without requiring a prior handshake for

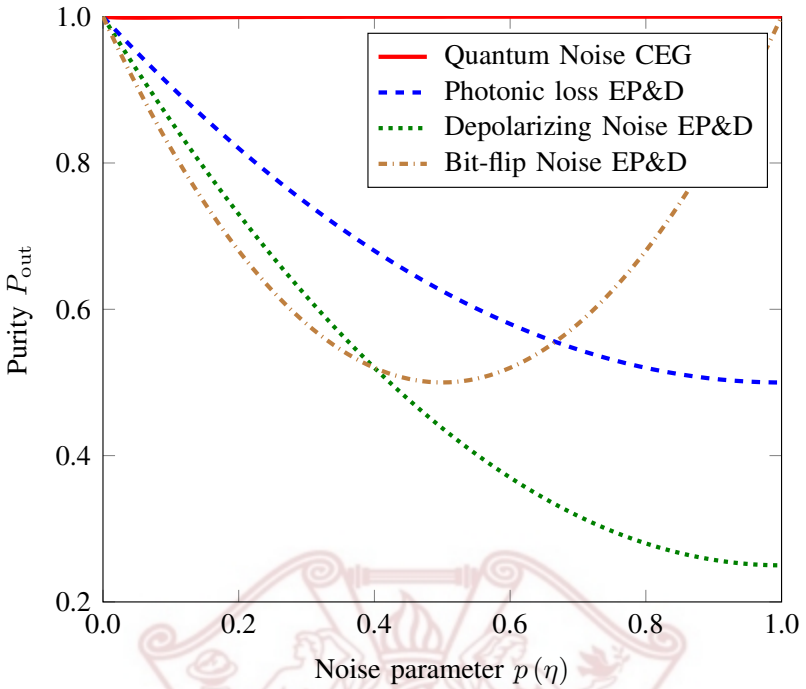


Figure 5.3: Purity of the output states for different noise models.

quantum information transfer, unlike previous entanglement distribution schemes. On the flip side, the counterfactual setup is probabilistic due to the possibility of a photon ending up in the channel. We have discussed the success probability of our scheme in 5.2.4.

5.2.2 Polarization DOF Noise in DCC Protocols

The presence of noise on the quantum channel decoheres the quantum state which directly affects the counterfactual communication. We first discuss the noise affecting the polarization property of the photon over the channel. For this purpose, we consider the depolarizing noise, dephasing noise, and, bit-flip noise models in the computational basis. Note that for all the noise models, we consider $M = 20$, $N = 100$, and the same noise on

both directions of the two-way channel (Alice to Bob and Bob to Alice) for simulations. In each cycle of the H-CQZ$_{\mathrm{QNM}}$ gate, the polarization DOF noise in the quantum channel corrupts the H-polarized photon component in $|2\rangle_{\mathrm{path}}$. For a generalized polarization DOF noise, ith Kraus operator for Alice's photon is $\mathcal{K}_{\mathrm{A}_i}$. The total noise operator is

$$\begin{aligned}\mathcal{K}_i = &|\downarrow\rangle_{\mathrm{B}}\langle\downarrow|_{\mathrm{B}} \otimes \mathcal{K}_{\mathrm{A}_i} \otimes |2\rangle_{\mathrm{path}}\langle 2|_{\mathrm{path}} \\ &+ |\downarrow\rangle_{\mathrm{B}}\langle\downarrow|_{\mathrm{B}} \otimes \boldsymbol{I}_{\mathrm{A}} \otimes |0\rangle_{\mathrm{path}}\langle 0|_{\mathrm{path}} \\ &+ |\downarrow\rangle_{\mathrm{B}}\langle\downarrow|_{\mathrm{B}} \otimes \boldsymbol{I}_{\mathrm{A}} \otimes |1\rangle_{\mathrm{path}}\langle 1|_{\mathrm{path}} \\ &+ |\uparrow\rangle_{\mathrm{B}}\langle\uparrow|_{\mathrm{B}} \otimes \boldsymbol{I}_{\mathrm{A}} \otimes \boldsymbol{I}_{\mathrm{path}}, \end{aligned} \tag{5.12}$$

where the first quantum system is the qubit QAO, second is polarization qubit and the third is path qutrit.

Dephasing Channel

We first consider the effect of dephasing channel noise in the polarization degree of freedom on our setup. Generally, the dephasing noise modifies a state $\boldsymbol{\rho}$ as

$$\boldsymbol{\rho}_{\mathrm{out}} = \sum_{i=0}^{1} \boldsymbol{K}_{\mathrm{A}_i} \boldsymbol{\rho} \boldsymbol{K}_{\mathrm{A}_i}^{\dagger}, \tag{5.13}$$

where $\boldsymbol{K}_{\mathrm{A}_0} = \sqrt{1-p}\boldsymbol{I}, \boldsymbol{K}_{\mathrm{A}_1} = \sqrt{p}\sigma_z$ and p is dephasing noise parameter and $0 \leq p \leq 1$. Here $\boldsymbol{I}$ is the identity operator on the quantum system while σ_z is the Pauli-Z quantum operator on a qubit. One primary advantage of the counterfactual setup is that the photonic component in the channel has no entropy because it is always H-polarized. Assuming we have the knowledge of the preferred polarization state over the channel, the PR$_{\mathrm{QNM}}$ in Fig 5.1 converts the H-polarized channel component to the preferred polarization and re-converts it back to H once it returns from Bob. Since only the preferred polarization basis enters the channel, therefore it will not be affected by the dephasing noise. For the case of dephasing noise in computation basis where $\boldsymbol{K}_{\mathrm{A}_1} \propto \sigma_z$ if the horizontal polarization

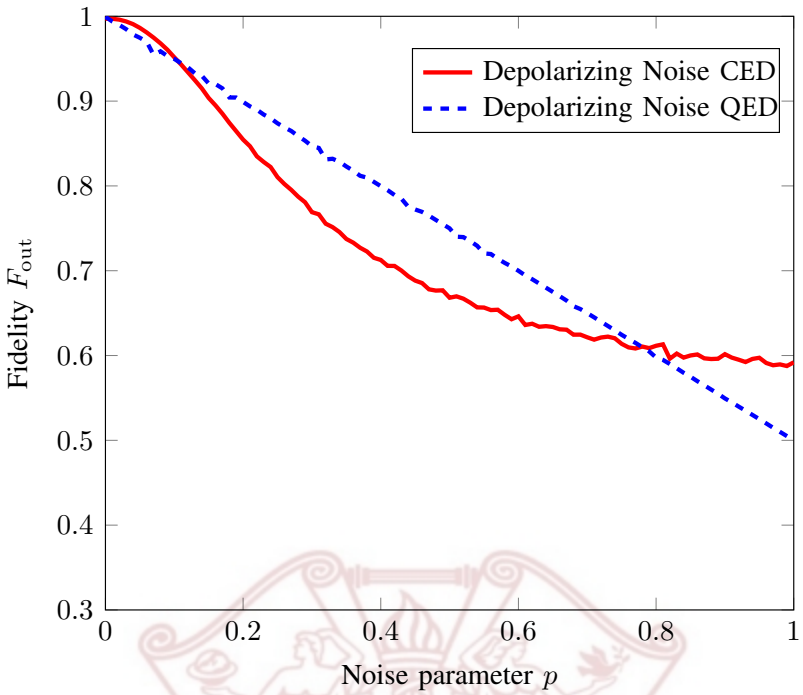


Figure 5.4: Fidelity of the distributed entangled state for depolarizing noise.

corresponds to the lower level (level-0), the preferred basis is H-polarized [47]. Therefore, PR_{QNM} will not cause any rotation. Hence, the effect of the dephasing channel noise is nullified.

In comparison to our setup, conventional entanglement distribution is two-stepped: entanglement preparation and distribution (EP&D). The distribution involves one particle traveling over the channel which is susceptible to dephasing.

Bit-flip Noise

Similar to dephasing, bit-flip noise is generally represented by the Kraus operators $\boldsymbol{K}_{\text{A}_0} = \sqrt{1-p}\boldsymbol{I}, \boldsymbol{K}_{\text{A}_1} = \sqrt{p}\sigma_x$, where σ_x is the Pauli-X operation. Once the photon component returns from the channel, the H-polarized channel component has been transformed into

the mixedness of horizontal and vertical polarized components under the bit-flip operation. Here again, we utilize the advantage associated with the $\mathrm{PBS}^{\mathrm{H}}_{\mathrm{QNM}}$ and $\mathrm{D}_{\mathrm{QNM}}$ which absorb the V-component. Although this absorption removes the probabilistic nature of the noise, the off-diagonal terms in the density matrix ρ are still updated. This leads to a rotation proportional to the probability of noise but the purity is not affected unlike previous schemes, i.e., purity

$$P_{\mathrm{out}} = \mathrm{tr}\left(\boldsymbol{\rho}^2_{\mathrm{out}}\right) = 1. \tag{5.14}$$

But it drifts away from the ideal output $\sigma = |\xi\rangle\langle\xi|$, where $|\xi\rangle = 1/\sqrt{2}\left(|{\downarrow}\rangle_{\mathrm{B}}|\mathrm{H}\rangle_{\mathrm{A}} + |{\uparrow}\rangle_{\mathrm{B}}|\mathrm{V}\rangle_{\mathrm{A}}\right)$. That is

$$F_{\mathrm{out}} = \mathrm{tr}\left(\sqrt{\sqrt{\boldsymbol{\rho}_{\mathrm{out}}}\boldsymbol{\sigma}\sqrt{\boldsymbol{\rho}_{\mathrm{out}}}}\right)^2 < 1. \tag{5.15}$$

This provides us with a unique situation, where we can correct the final state through a reversal unitary operator $U_p^\dagger$ based on the probability p of bit-flip noise. For identifying this parameter p, channel/process tomography techniques can be employed [118]. This is unlike the case of general quantum communication, where mixedness (decrease in purity) cannot be removed without using and sacrificing copies of the output states via purification [57]. Figure 5.2 shows the fidelity (without $\mathrm{PR}_{\mathrm{QNM}}$ rotation) of the counterfactually entangled state. Each line in the figure shows the mean performance of the 10^3 randomly generated qubit states according to the Haar measure. Here, the fidelity of this state scales linearly with the fidelity of the shared entangled state. Figure 5.3 shows the purity of counterfactual entanglement generation in comparison to an information-carrying quantum particle in EP&D. Without $\mathrm{PR}_{\mathrm{QNM}}$ rotation, the counterfactual setup has less output state fidelity, however, the output state is still retrievable given the channel state information unlike conventional quantum setup under bit-flip channel noise. Furthermore, given the information that $\boldsymbol{K}_{\mathrm{A}_1} \propto \sigma_x$, if horizontal polarization corresponds to level-0, $\mathrm{PR}_{\mathrm{QNM}}$ will rotate the state to the $\left(|\mathrm{H}\rangle + |\mathrm{V}\rangle\right)/\sqrt{2}$, which is unaffected under the bit-flip channel

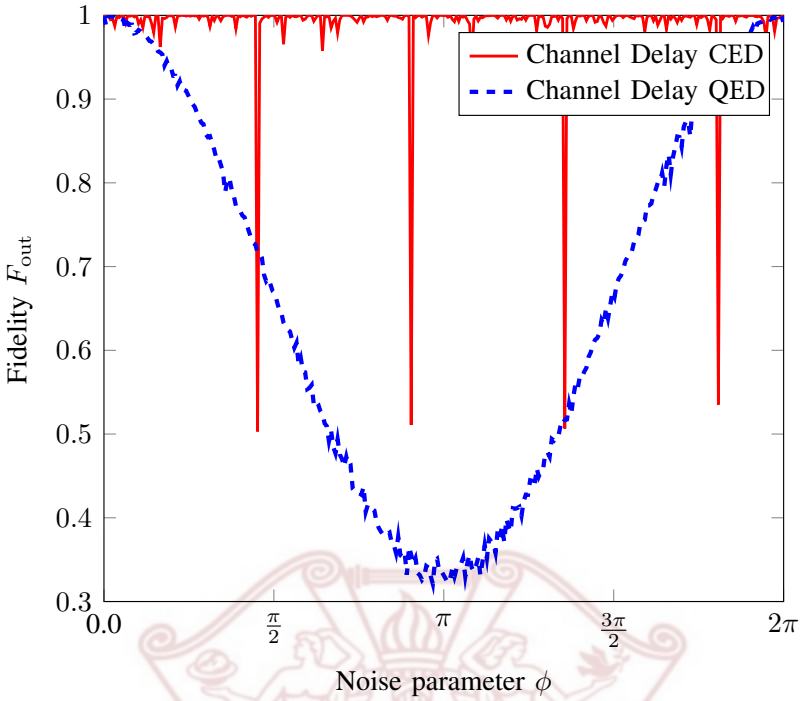


Figure 5.5: Fidelity of the distributed entangled state for channel delay noise.

noise. In case both dephasing and bit-flip noise exist on the channel, we can only counter one of them through PR_{QNM} as described in the depolarizing noise part.

Depolarizing Noise

The depolarizing noise modifies a state $\boldsymbol{\rho}$ as

$$\boldsymbol{\rho}_{\text{out}} = (1-p)\,\boldsymbol{\rho} + p\pi, \tag{5.16}$$

where $\pi = \boldsymbol{I}/d$ is a maximally mixed state for d- dimensional system, p is the depolarizing noise parameter and $0 \leq p \leq 1$.

As discussed before, if PR_{QNM} does not cause any rotation, the dephasing component will not lead to any effect for our setup. However, the bit flip noise along the X and Y axis of the Bloch sphere rotate the post-operation QAO state based on the parameter

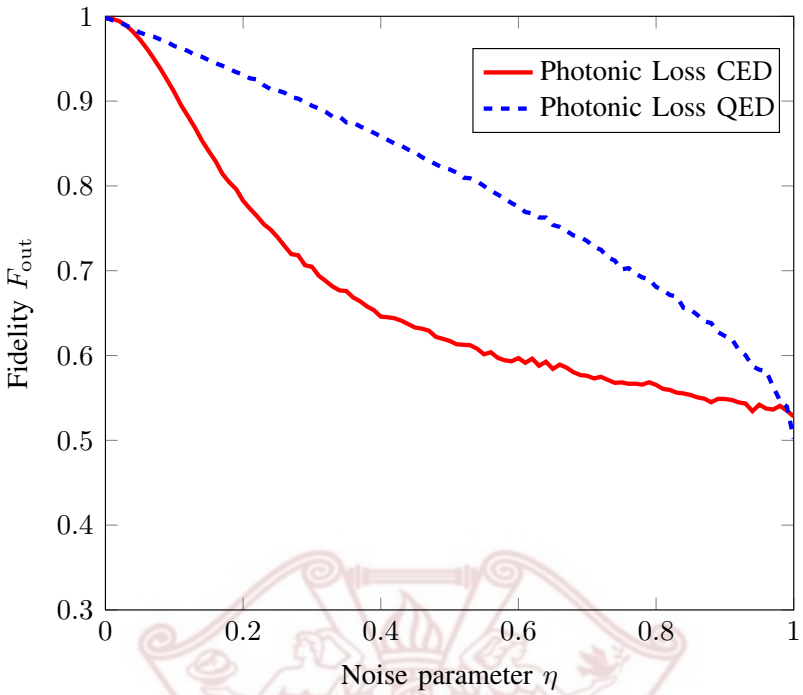


Figure 5.6: Fidelity of the distributed entangled state for photonic loss.

p. Figure 5.4 shows the fidelity of output states for depolarizing noise. Similar to bit-flip noise, although output fidelity is less for the counterfactual system, the possibility of state retrieval due to $P_{\text{out}} = 1$ (see Figure 5.3) makes it more suited than conventional entanglement distribution given channel state information.

5.2.3 Path DOF Noise Models

We now discuss the noise incorporated into the path degree of freedom. Any optical quantum interferometric suffers from the following three noise types: i) phase diffusion, ii) interferometric invisibility, and iii) photonic loss and dispersion [113]. The former two result from the change in effective optical length in one path and subsequent interference; while the latter results from photonic component loss in the channel path.

Change of Effective Path Length

In case of a channel delay, the effective change in length leads to a phase diffusion map provided by $\boldsymbol{R}_{\theta_\ell}$ in the path DOF of the quantum system, where

$$\boldsymbol{R}_{\theta_\ell} = \begin{pmatrix} e^{\frac{-i\theta_\ell}{2}} & 0 \\ 0 & e^{\frac{i\theta_\ell}{2}} \end{pmatrix}. \tag{5.17}$$

Assuming i) the channel delay leads to uniformly distributed rotation angle $\theta_\ell \in [-k\pi, k\pi]$ $\forall k \in \mathbb{Z}$ and, ii) θ_ℓ remains constant for the duration of a single H-CQZ$_{\text{QNM}}$ operation, it modifies a state $\boldsymbol{\rho}$ as [113]

$$\boldsymbol{\rho}_{\text{out}} = \frac{1}{2\pi} \int_{\theta_\ell} p_{\theta_\ell}(\theta_\ell)\, \boldsymbol{R}_{\theta_\ell} \boldsymbol{\rho} \boldsymbol{R}_{\theta_\ell}^{\dagger} d\theta_\ell, \tag{5.18}$$

For the combined photon-QAO system, the photon component in the channel $|\text{H(V)}\rangle_{\text{A}} |2\rangle_{\text{path}}$ interacts with the present $|\uparrow\rangle_{\text{B}}$ and absent $|\downarrow\rangle_{\text{B}}$ components of QAO. The interaction between QAO present component $|\uparrow\rangle_{\text{B}}$ with $|\text{H(V)}\rangle_{\text{A}} |2\rangle_{\text{path}}$ results in $|\text{H(V)}\rangle_{\text{A}} |2\rangle_{\text{path}}$'s absorption. While the interaction between QAO absent component $|\downarrow\rangle_{\text{B}}$ with $|\text{H(V)}\rangle_{\text{A}} |2\rangle_{\text{path}}$ reflects the photon. In the latter case, the randomized rotation due to channel delay is applied between the $|1\rangle_{\text{path}}$ and $|2\rangle_{\text{path}}$ arms of the inner interferometer. If the photon component is reflected, the inner interferometer acts as Michelson's interferometer. In this case, once the two reflected components in $|1\rangle_{\text{path}}$ and $|2\rangle_{\text{path}}$ meet in the inner Michelson interferometer, the channel delay information gets encoded into the polarization DOF. Therefore, without loss of generality, for ith Kraus operator, we consider $\boldsymbol{R}_{\theta_{i_{\text{path}_{1,2}}}}$ being applied between the paths $|1\rangle_{\text{path}}$ and $|2\rangle_{\text{path}}$ as

$$\begin{aligned} \boldsymbol{K}_i = & |\downarrow\rangle_{\text{B}} \langle\downarrow|_{\text{B}} \otimes \boldsymbol{I}_{\text{A}} \otimes \boldsymbol{R}_{\theta_{i_{\text{path}_{1,2}}}} \\ & + |\downarrow\rangle_{\text{B}} \langle\downarrow|_{\text{B}} \otimes \boldsymbol{I}_{\text{A}} \otimes |0\rangle_{\text{path}} \langle 0|_{\text{path}} \\ & + |\uparrow\rangle_{\text{B}} \langle\uparrow|_{\text{B}} \otimes \boldsymbol{I}_{\text{A}} \otimes \boldsymbol{I}_{\text{path}}. \end{aligned} \tag{5.19}$$

Considering this, the effect of channel delay is to cause a path mismatch between the two arms of the inner interferometer for the case when QAO is absent. This causes periodic sudden drops in fidelity whenever the channel component of the photon is reflected back by Bob, as evident in Figure 5.5. For given values of M and N, fidelity within a tolerance level could be achieved in this case even if only approximate channel state information is available. Unlike the counterfactual case, conventional entanglement distribution through the EP&D method has a progressive drop in fidelity. For the case where deviation in path length corresponds to $\phi = \pi$, fidelity is 0.

Photonic Loss/Dispersion in Channel

In a lossy counterfactual interferometric setup, fictitious polarization beam splitters in the channel account for the photonic loss and dispersion in the channel [113]. In the case of this dispersion, the component in the channel disperses and is replaced by a vacuum state. For the counterfactual setup, we shall treat such dispersion as equivalent to the absorption of channel components due to noise. This corresponds to an amplitude damping channel with Kraus operators given as

$$\mathcal{K}_{\text{path}_0} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\eta} \end{pmatrix}, \qquad \mathcal{K}_{\text{path}_1} = \begin{pmatrix} 0 & \sqrt{\eta} \\ 0 & 0 \end{pmatrix}, \tag{5.20}$$

where $\eta = 1 - e^{-\gamma t}$ is the decay probability and γ is the loss rate. For these Kraus operators, path_1 is the non-decaying entry and path_2 is the decaying entry. The generalized noise model will therefore be

$$\begin{aligned} \boldsymbol{K}_i = & \left|\downarrow\right\rangle_{\text{B}} \left\langle\downarrow\right|_{\text{B}} \otimes \boldsymbol{I}_{\text{A}} \otimes \mathcal{K}_{\text{path}_i} \\ & + \left|\downarrow\right\rangle_{\text{B}} \left\langle\downarrow\right|_{\text{B}} \otimes \boldsymbol{I}_{\text{A}} \otimes \left|0\right\rangle_{\text{path}} \left\langle 0\right|_{\text{path}} \\ & + \left|\uparrow\right\rangle_{\text{B}} \left\langle\uparrow\right|_{\text{B}} \otimes \boldsymbol{I}_{\text{A}} \otimes \boldsymbol{I}_{\text{path}}. \end{aligned} \tag{5.21}$$

Figure 5.6 shows the fidelity of the H-CQZ$_{\text{QNM}}$ operation in the presence of photonic losses for both cases. In comparison to conventional schemes, phase diffusion does affect

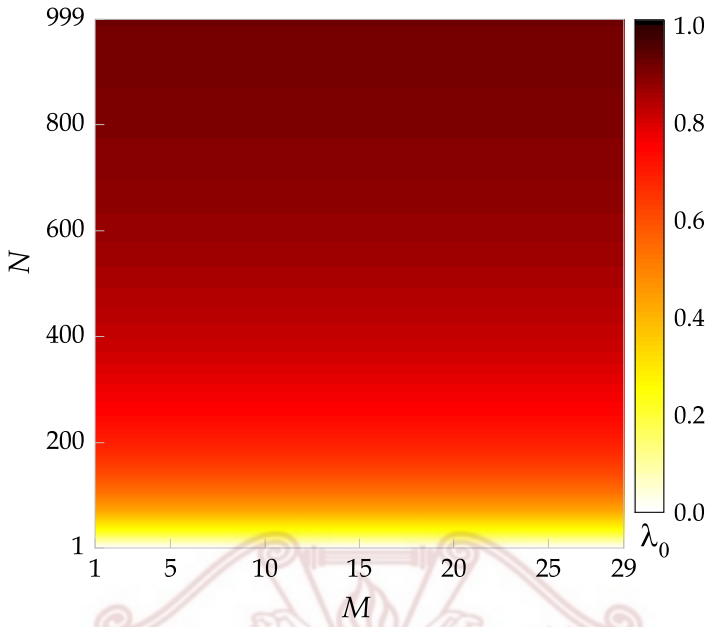


Figure 5.7: Probability of successful classical communication of logical 0 with AO absent.

the fidelity of the counterfactual setup. Although the loss of fidelity is more than the conventional setup, output state recovery is possible given the channel state information due to no mixedness (see Figure 5.3).

5.2.4 Probability of success for H-CQZ$_{\mathrm{QNM}}$ operations

For each of the three H-CQZ$_{\mathrm{QNM}}$ operations, if the photon ends up in the channel, the counterfactuality is lost. Therefore, we need to redo that H-CQZ$_{\mathrm{QNM}}$ operation. The success probability for H-CQZ$_{\mathrm{QNM}}$ operation with AO absent is λ_0 given by [52]

$$\lambda_0 = \cos^{2M} \theta_M, \tag{5.22}$$

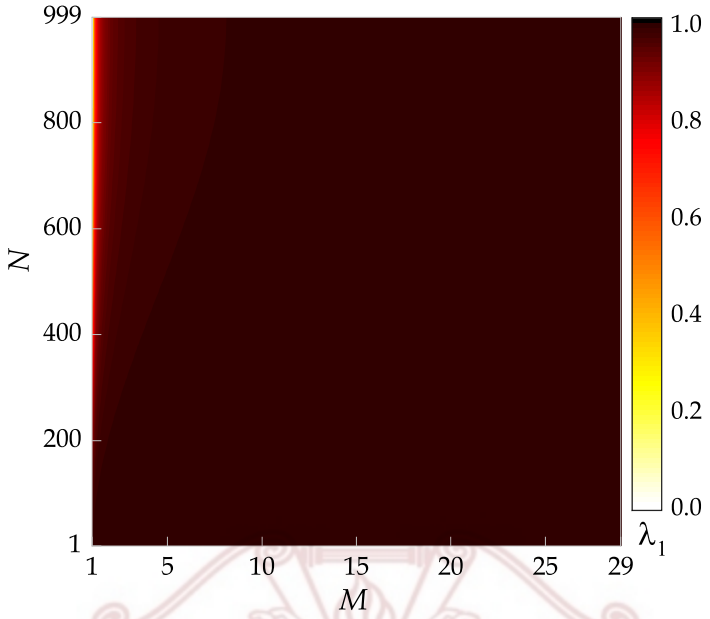


Figure 5.8: Probability of successful classical communication of logical 1 with AO present.

while for AO present case, we have

$$\lambda_1 = \prod_{m=1}^{M} \left[1 - \sin^2(m\theta_M) \sin^2\theta_N\right]^N . \tag{5.23}$$

For entanglement generation with QAO, the probability of success is [76]

$$\lambda_2 = \left(1 - \frac{1}{2}\sin^2\theta_M\right)^M \prod_{m=1}^{M} \left[1 - \frac{1}{2}\sin^2(m\theta_M)\sin^2\theta_N\right]^N , \tag{5.24}$$

Figures 5.7, 5.8 and 5.9 show the successful probability of H-CQZ$_{\mathrm{QNM}}$ operation as a function of outer cycles M and inner cycles N of H-CQZ$_{\mathrm{QNM}}$ gate for AO absence, AO presence and QAO in the channel respectively.

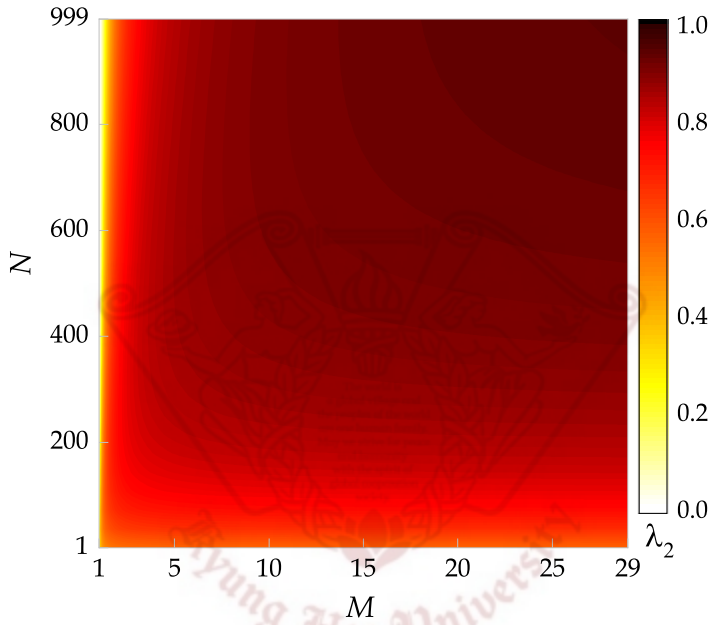


Figure 5.9: Probability of successful entanglement distribution with QAO in the superposition state $\frac{1}{\sqrt{2}}(|\uparrow\rangle_{\mathrm{B}} + |\downarrow\rangle_{\mathrm{B}})$.

5.3 Conclusion

We have investigated and enhanced the robustness of the counterfactual entanglement distribution of our counterfactual consensus scheme based on the modified DCC. The modification allows us to achieve high-fidelity entanglement distribution under noisy conditions compared to the conventional setup. We have shown that our modified DCC-based scheme is robust against channel delay and dephasing noise. While for photonic loss, depolarizing, and bit-flip noise, it is possible to retrieve the original state given only the channel state information. Furthermore, our scheme does not require any *a priori* shared phase reference which is a necessity for conventional quantum schemes.

Future works may include an experimental implementation of our proposed setup and investigating the hardware requirements and considerations for scaling up this setup to a network level.

Chapter 6

Comparative Robustness of Previous Quantum Consensus Algorithms And Counterfactual Consensus

At the heart of the coordinated behavior of distributed network nodes is the information consensus including clock synchronization.

Currently, most consensus mechanisms for distributed networks (e.g., in Blockchain consensus) employ classical BA-based practical Byzantine fault tolerance (PBFT) algorithm or its derivatives for countering malicious nodes in consensus networks [119]. QBA schemes allow better fault tolerance than PBFT and allow lower communication complexity, making them promising candidates for network consensus. However, in the NISQ era, their performance has not been evaluated for this task in a practical network setting. As discussed in the last chapter, the problem of BA consensus can be reduced to the problem

of sharing private lists in the network [40].

Quantum resources provide many nonclassical features that have been utilized for groundbreaking works in secure communication. Researchers have recently provided many quantum algorithms to achieve BA using quantum resources such as entanglement and coherence. If the BA condition is relaxed to include the option of all loyal parties aborting, the quantum BA schemes can tolerate up to half faulty participants in the network. Hence, unlike classical methods, they can provide an agreement for a tri-partite network with one faulty node. These consensus mechanisms have been employed for quantum tasks such as clock synchronization and secret sharing [106, 108, 120].

In this chapter, we evaluate the performance of various QBA protocols in terms of their scalability, security, and decentralization for practical network consensus. In particular, we investigate the robustness of these algorithms for practical NISQ devices. The main contributions of this chapter can be summarized as follows.

- *Realization of Practical NISQ Era QBA Networks:* Quantum schemes provide better fault tolerance and communication complexity; however, they will be prone to quantum noise in the NISQ era devices. For consideration of these quantum algorithms for practical blockchain networks, quantum noise in the networked setting is inevitable. Furthermore, no theoretical analysis of the quantum noise exists for these QBA schemes to date. Therefore, there is a need to investigate these QBA algorithms in practical NISQ-era networked settings for the aforementioned performance measures. In particular, the analysis of such algorithms for noisy quantum processor memory and noisy quantum channels for different noise models and noise levels is essential so we can utilize them for practical blockchain consensus. For this purpose, we consider qubit decoherence and depolarizing noise in quantum processors and noisy quantum fiber-optic channels and evaluate the performance of QBA algorithms.

- *Emulation of QBA Networks for Near-Practical Applications:* Quantum computers and simulators have existed for some time now, but there were no quantum networks available for implementing quantum network algorithms until recently. Although we can simulate network protocols like teleportation on quantum computers/simulators, they do not carry the essence of network settings such as impacts of the quantum handshake, fiber-optic delays, and change of qubit modality from static to flying qubits. Chien et al. used a localized experimental setup to demonstrate the QBA; however, it does not provide information about its practicality in a networked setting for Blockchain consensus [121]. Moreover, the experimental settings in [40, 120] provide results for a particular setting of node distance, noise model, and the number of parties and cannot be used for generalized results. Recently, researchers at QuTech proposed a discrete event quantum network simulator (NetSquid) which allows emulating network applications while considering the impacts of practical considerations on them [41]. Netsquid is currently being augmented to an actual quantum network through the *Quantum Network Explorer* [122]. We have used Netsquid to emulate the practical NISQ-era QBA systems as close as possible to practical experiments.

- *Consideration of QBA in the Absence of Quantum Handshake:* Quantum devices require shared phase definitions in addition to sharing the reference frames [107]. This need is a critical bottleneck for distributed quantum computation, clock synchronization, and QKD networks [32, 107]. In practical settings, the phase definitions of quantum devices can change over time, leading to a nonfungible source of quantum decoherence. We not only show how this affects QBA systems but also identify which QBA algorithms are best suited for this problem.

- *Performance Evaluation of QBA Algorithms:* We evaluate the error rates in list distribution for each QBA protocol and compare their performance. We observe that quantum consensus algorithms have better malicious fault tolerance (security),

lower scalability, and comparable decentralization when compared to their classical counterparts. While counterfactual BA scheme is the most scalable among them due to its robustness against dephasing shown in the previous chapter.

6.1 Quantum Consensus Algorithms

To compare different QBA algorithms, we first discuss the entanglement-based schemes for list distribution before discussing entanglement-free scenarios that utilize quantum coherence. We will evaluate the performance of these protocols in terms of the security, scalability, and decentralization for blockchain consensus.

6.1.1 Entanglement-Based Quantum Consensus

The first quantum BA algorithm utilized a three-qutrit Aharnov state shared between the three participants [37]

$$\begin{aligned} |\psi\rangle \quad &= \frac{1}{\sqrt{6}}(|0,1,2\rangle + |1,2,0\rangle + |2,0,1\rangle \\ &\quad - |0,2,1\rangle - |1,0,2\rangle - |2,1,0\rangle). \end{aligned} \tag{6.1}$$

However, it utilized qutrits which are not readily available and controllable in the NISQ era devices. Therefore, for NISQ-era quantum networks, we will consider only qubit-based procedures [123].

QKD-Based QBA

QKD is the protcol for distributing secret keys between two parties [117]. Two QKD channels between three parties can share private correlated lists between them. For this purpose, we consider the E91 protocol based on shared enlargement due to its superior performance over the original BB84 scheme [117, 124]. In this case, Alice prepares two

copies of an entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{6.2}$$

She keeps one particle of each copy to himself and shares the other particle of the first (second) entangled state to Bob_1 (Bob_2) over the optical fiber. Once entanglement distribution has been established, each party applies local measurement on their local qubits in either the computational (Pauli-Z) or the diagonal (Pauli-X) basis. Similar to QKD schemes, the parties then reveal their measurement basis, and if the bases agree, the private lists correspond to the measurement results.

Singlet-Based QBA

For singlet-based QBA, a quantum source distributes four-qubit singlet states [40]

$$\begin{aligned} |\phi\rangle \quad &= \frac{1}{2\sqrt{3}}\left(2\,|0011\rangle - |0101\rangle - |0110\rangle\right. \\ &\quad \left. - |1001\rangle - |1010\rangle + 2\,|1100\rangle\right). \end{aligned} \tag{6.3}$$

to the participants of the QBA. Alice receives two qubits while Bob_1 and Bob_2 receive one qubit each. Each party chooses a measurement basis and applies it to its local qubits. After measurement, all parties announce their measurement bases. If their measurement bases are the same, the measurement outcomes become private list entries. This singlet-based bit-valued decision was recently upgraded to multivalued BA through a d-dimensional entangled system [103].

From the perspective of decentralization, both entanglement-based systems involve local measurement by each of the participants; hence, they are fairly decentralized. Regarding security, the entanglement distribution procedure halts if an adversary intercepts a particle in the entangled states in (6.2) and (6.3) over the channel. Furthermore, the QKD-based scheme utilizes the unconditional security of the quantum cryptographic schemes. Therefore, these schemes outperform their classical counterparts in terms of security. In

terms of scalability, the entangled states are highly susceptible to channel noise, and the loss of a single particle from singlet or GHZ states leads to the entire distribution being rendered useless. As the number of participants increases, these schemes are increasingly prone to failure.

6.1.2 Entanglement-Free Quantum Consensus

We now investigate the private correlated list distribution protocol using an unentangled qutrit or qudit to achieve BA [24, 106, 120]. This protocol utilizes a single K-dimensional qudit

$$|\xi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |k\rangle , \tag{6.4}$$

where the number of dimensions corresponds to the number of parties involved in the scheme. The first node (Alice) prepares the qudit, encodes her choice of basis $\mathfrak{b}$ through unitary encoding

$$\boldsymbol{V} = |0\rangle \langle 0| + \sum_{k=1}^{K-1} e^{i2\pi \mathfrak{b}/K} |k\rangle \langle k| , \tag{6.5}$$

and her choice of secret private list entry $\mathfrak{s}$ through

$$\boldsymbol{U} = \sum_{k=0}^{K-1} e^{i2\pi k \mathfrak{s}/K} |k\rangle \langle k| , \tag{6.6}$$

respectively, and sends it to the second party (Bob_1). The second party similarly encodes its choices and sends the qudit to the next Bob_2. Once the last party, Bob_{K-1}, receives the state, he applies its encoding and measures the qudit in Fourier basis $\{|\xi\rangle \langle \xi| , I - |\xi\rangle \langle \xi|$. If the measured result is $|\xi\rangle$, each party reveals the basis choice $b_i \ \forall i \in K$ in random order. If the choice of basis $b_i \mod K = 0$, the private list entries are correlated.

The advantage of using a qudit-based scheme is that it increases the scalability of the network compared to entanglement-based methods because it employs only one detector.

However, this also leads to lesser decentralization because only a single party performs the measurement. Furthermore, the single qudit traveling over the channel is more susceptible to malicious attacks due to the entire unentangled quantum system available to the adversary, thereby reducing its security [62].

Multi-Qubit Implementation of Qudit-Based QBA

As discussed in the previous section, qudit-based QBA is the most practical QBA candidate due to its better scalability. However, for the current era of NISQ devices, the generation and manipulation of qudits suffer from practical constraints, including unavailability and limited control [41,125]. Therefore, we utilize a multiqubit system that mimics the qudit with similar network architecture. To generate the state (6.4) for K-partite system, we use $\lceil \log_2 K \rceil$ qubits, where each qubit is in the maximal superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The $\boldsymbol{U}$ operator is decomposable to single-qubit operations but the $\boldsymbol{V}$ operator requires joint evolution of all qubits at the local processor. For implementation on the NISQ era quantum network, we consider that the qubits both arrive at the same time and that the processors can employ two-qubit operations.

6.2 Quantum Noise in NISQ Networks

For the NISQ era, quantum noise has been the fundamental bottleneck in implementing practical quantum computation and communication systems. For practical realizations of consensus algorithms, quantum noise will degrade the quality of the qubits over the channel and in the quantum processor memory. The noise can degrade speakable and/or unspeakable information carried by the quantum processor network. In this section, we investigate the performance of the three qubit-based QBA protocols against both unspeakable (nonfungible) and speakable (fungible) quantum noise [107]. The nonfungible quantum noise is the absence of the shared quantum phase reference between the distributed processors,

an additional reference frame required for distributed quantum computation alongside the shared inertial reference frame, while speakable quantum noise constitutes channel and local quantum noise affecting the qubit's information-carrying degree of freedom over the optical fiber or local quantum processor memory. Our analysis is limited not only to quantum networks but also encompasses the investigation of the QBA schemes for quantum networks.

6.2.1 Quantum Noise in Nonfungible Information—Absence of Shared Phase Reference

For the entanglement-assisted quantum consensus schemes, one party (say Alice) prepares the entangled state locally and then shares one particle of each entangled state with Bob [24, 32]. Each party measures the qubit, either in the Pauli-Z or Pauli-X basis at random. Recently, entanglement purification has been identified as a possible solution to counter the absence of the shared phase reference for entanglement distribution [32, 57]. In this procedure, using the quantum circuit method, Bennet et al.'s entanglement purification is iteratively used to obtain singlets in the local basis [57]. However, it requires n entangled states and leads to the loss of half population of entangled states in each purification cycle. Furthermore, the fidelity F_n of the entangled pairs after n rounds of purification is [57]

$$F_n = \frac{F_{n-1}^2 + \frac{1}{9}\left(1 - F_{n-1}\right)^2}{F_{n-1}^2 + \frac{2}{3}F_{n-1}\left(1 - F_{n-1}\right) + \frac{5}{9}\left(1 - F_{n-1}\right)^2}, \tag{6.7}$$

where F_{n-1} is the fidelity after the $(n-1)$th round of purification. After the nth round, the X entangled states are *reduced* to $X/2^n$ singlets. Furthermore, the probability of discarding the purification results for a round is *nonzero.*

For the entanglement-free scheme, the qubits are prepared locally at Alice and undergo diagonal operator evolution at other parties. The last party measures the multi-qubit state in the Fourier basis, which is a non-computational-basis measurement. Therefore, the absence of shared phase reference (SRF) becomes a problem.

For counterfactual consensus, only local parties have control over the quantum evolution of their quantum systems. In the setup of H-CQZ gate, the QAOs at the central node's end do not evolve during the HCQZ operation, and the horizontally polarized photon at each Bob_i undergoes only local quantum evolution. The only action by the central party's QAOs on the photon is either reflection or absorption of the H-component on the channel. Therefore, our setup allows independent local definitions of phase reference and is practical for plug-and-play networks without requiring an initial handshake for quantum information transfer, unlike previous quantum QBA schemes.

6.2.2 Quantum Noise in Fungible Information

In addition to the desynchronization of phase reference, the quantum processor and fiber-optic links may have quantum noise, causing qubit decoherence. We consider fiber-optic quantum dephasing noise. For NISQ quantum networks, a qubit or quantum wave-function in transit over a fiber-optic channel undergoes dephasing for the duration of its transit. For a qubit in the state ρ, it undergoes the noisy transition to

$$\sigma = (1-p)\rho + p\sigma_z\rho\sigma_z, \tag{6.8}$$

where σ_z is the Pauli-Z operator on the qubit and p is the dephasing noise parameter.

6.3 NISQ Network Setup for QBA Algorithms

We now investigate the noise-robustness of the three qubit-based QBA schemes. For our analysis, we utilize the NetSquid network simulator for evaluating the error rate in list distribution for QBA [41]. Netsquid is explicitly built to emulate a quantum network. It models the network by NISQ-era quantum devices connected by fiber-optic links for classical and quantum information transfer. Utilizing the Netsquid, we can capture the protocol's behavior as close to the actual practical implementation as possible instead of

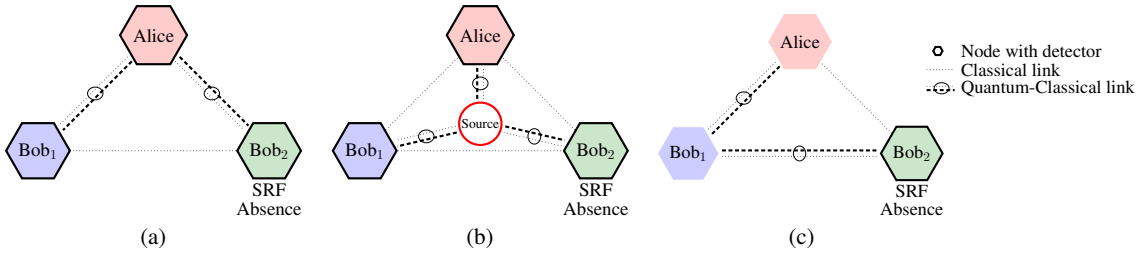


Figure 6.1: Network architecture for three QBAs: (**a**) QKD-based QBA, (**b**) singlet-based QBA, and (**c**) multiqubit-based QBA. The classical links are pairwise, while quantum links form a chain. We assume that Bob_2 can have local memory noise.

simplistic localized simulation using a quantum or classical computer. Recently, Chien et al. utilized a general quantum circuit simulator to simulate the Byzantine agreement. This result, however, is obtained by running the circuit locally using static qubits such as superconducting qubits, ignoring any communication-related issues. Furthermore, with the development of *Quantum Network Explorer* by the same team, soon we will be able to implement NetSquid emulation in an actual open-source quantum network directly [122].

We have analyzed our results for tripartite networks with the two aforementioned cases: a) absence of shared phase reference and b) dephasing over the fiber-optic. The tripartite case is the most common consideration for the Byzantine agreement problems, in which the quantum algorithm can solve QBA if one party is faulty, unlike classical algorithms. By solving the three-party case, the solution can be generalized to an arbitrary number of parties with $t < n/2$ fault tolerance, where t denotes the number of faulty parties and n denotes the total number of parties. Figure 6.1 shows the network connection of QKD, singlet-based, and multiqubit-based schemes that we deploy in the NetSquid network simulator and provide the codes in the *Github repository* in [126]. The simulation parameters are listed in Table 6.1.

We model quantum and classical connections as fiber-optic channels that experience

Parameters	**QKD**	**Singlet State**	**Qudit**
Quantum State	two copies of entangled state	four-qubit singlet state	multiqubit state
Third-Party Source	✗	✔	✗
Classical Connections	pairwise authenticated channel	pairwise authenticated channel	pairwise authenticated channel
Quantum Connections	two quantum channels from Alice	pairwise from source to all parties	chain connection from first to the last party
Quantum Processor Capability	Hadamard gate, CNOT gate, measurement in Pauli-Z or Pauli-X basis	measurement in Pauli-Z or Pauli-X basis	Hadamard, U, and V gate, measurement in Fourier basis

Table 6.1: System Setup Parameters.

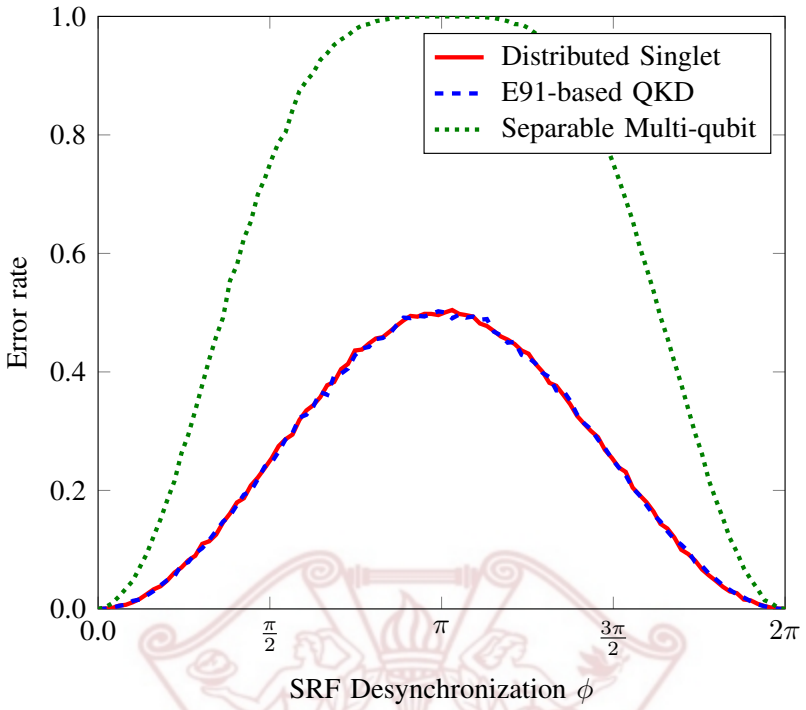


Figure 6.2: Impact of the absence of shared phase reference on the list distribution in the tri-partite network.

propagation delay or dephasing (the most practical decoherence models). The length of both classical and quantum are assumed to be four meters as we are considering a modular computing setup where each quantum processor is separated with a relatively small distance; hence, we do not consider any use of quantum repeater in the simulation. For the absence of a prior quantum handshake, we consider that Bob_2 lacks shared phase reference with other nodes. We run the protocol until we obtain a list with a length of 100 entries for all parties for each noise parameter value p ranging from 0 to 1 and plot the average error rate against that particular noise value for 100 data average.

6.4 Discussion

Figure 6.2 shows the error rate in the private correlated lists as the phase definitions of Bob_2 desynchronize with other parties. As the desynchronization in the phase definitions increases, the error rate increases. The increase in error rate of the multiqubit scheme is more adverse because all qubits undergo the effects of desynchronized phase definitions when measured, unlike entanglement-based QBA schemes where the qubit measured at Bob_2 is the only one experiencing noise effects. It becomes maximum for the case where the X-axis of Bob_2's Bloch sphere aligns with the Y-axis of Alice and Bob_1's Bloch sphere. From thereon, due to the circular nature of phase definition, the error begins to reduce, and for phase desynchronization $2x\pi$, $\forall x \in \mathbb{Z}$, the phase definitions are synchronized and lead to no error.

For counterfactual consensus, only local parties have control over the quantum evolution of their quantum systems. Therefore, our setup allows independent local definitions of phase reference without introducing any errors.

Figures 6.3 shows the case of dephasing noise on the qubits as they traverse over the fiber-optic channels. The effects are very similar to the case of desynchronization in phase definition. Again, the noise has the most adverse impact on the multiqubit case because the qubits have to travel from one party to the next. For each noisy link, the noise gets accumulated since the qudit is measured only at the last node. For QKD-based QBA, the nodes wait till they receive an acknowledgment from all parties. The additional duration for which qubit resides at the node increases the error rate for QKD compared to the singlet. Since we consider all quantum channels to be noisy, more qubits will undergo quantum noise, as apparent in comparing figures for local and channel noise.

One primary advantage of the counterfactual setup is that the photonic component in the channel has no entropy because it is always H-polarized. Assuming we have the knowledge of the preferred polarization state over the channel, the PR_{QNM} in the previous

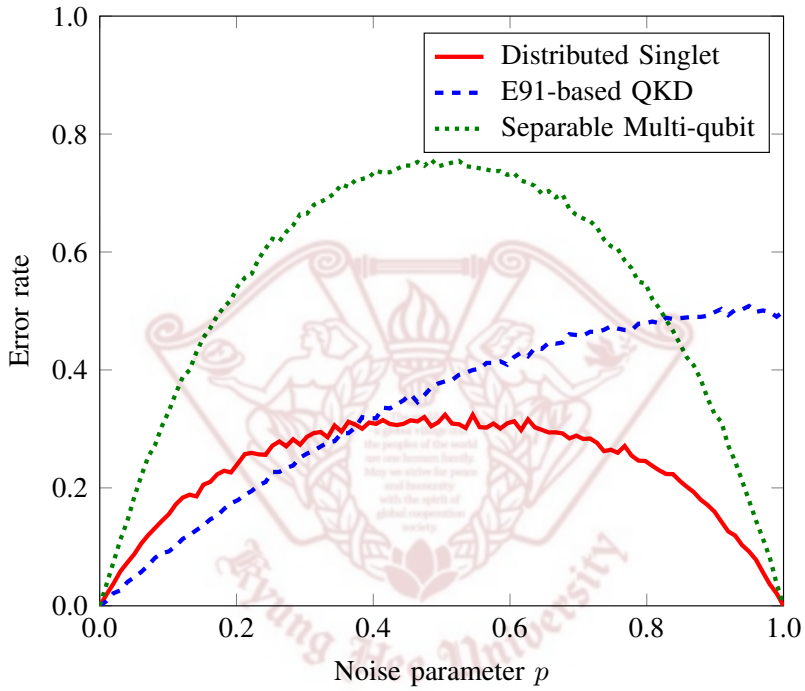


Figure 6.3: Impact of the optic fiber dephasing noise on the list distribution in the tripartite network.

chapter converts the H-polarized channel component to the preferred polarization and reconverts it back to H once it returns from Bob. Since only the preferred polarization basis enters the channel, therefore it will not be affected by the dephasing noise. For the case of dephasing noise in computation basis where $\boldsymbol{\mathcal{K}}_{\mathrm{A}_1} \propto \boldsymbol{Z}$, if the horizontal polarization corresponds to the lower level (level-0), the preferred basis is H-polarized [47]. Therefore, $\mathrm{PR}_{\mathrm{QNM}}$ will not cause any rotation. Hence, the effect of the dephasing channel noise is nullified.

6.5 Conclusions

In this paper, we have evaluated entangled and entanglement-free QBA algorithms against the counterfactual consensus for practical blockchain-enhanced distributed networks, such as sensor networks and modular quantum computing. We observe that in general, the counterfactual consensus has better noise robustness in comparison to its counterparts making it an ideal candidate for practical consensus. In general, all quantum consensus algorithms have better fault tolerance (and hence security) than classical algorithms. In the absence of quantum noise, entanglement-based consensus algorithms provide better security but do not scale very well. Though more scalable than other QBAs, the entanglement-free scheme offers less security and lesser decentralization because a single party performs measurement. In the presence of quantum decoherence, the fiber-optic quantum noise increases the generated list's error rate for previous quantum schemes. The effect of noise is more pronounced on multiqubit QBA because it degrades all the qubits at each of the noisy nodes, unlike the entanglement-based schemes, where the noise degrades only one qubit per noisy channel. Therefore, the entanglement-free QBA scheme is more affected than its counterparts. In comparison, the counterfactual scheme can be made robust against these two noise models as shown in Chapter 5. We observed that the error rate in list distribution is susceptible to the small levels of local qubit noise and

channel decoherence for non-counterfactual QBA schemes.

Chapter 7

Conclusion

In this chapter, we conclude our discussion, summarize the main results, and discuss some possible future directions. This dissertation investigated quantum synchronization and consensus for NISQ networks without shared phase reference. We have developed experimental setups based on multi-DOF entanglement and counterfactual communication for clock synchronization in a distributed network and derived some fundamental limits on the achievable precision with NISQ devices.

In chapter 2, we introduced a DQN for syntonizing distant oscillators at each node. Our proposed scheme did not require a prior quantum handshake or shared phase reference by requiring only diagonal quantum unitary operator evolution at distant nodes. We showed that the precision achievable in a node's LO syntonization is limited only by its local quantum decoherence. We provided the procedure of integrating a new node into the network based on its local quantum noise measure. This quantitative measurement of local decoherence allowed us to optimize our resources for LO resyntonization. Furthermore, we divided LO resyntonization into two stages, desynchronization detection, and LO resyntonization. This segregation allowed us to optimize the syntonization resources for each node in the presence of phase-covariant noise models.

In chapter 3, we employ the paradigm of counterfactual communication, which is based on interaction-free measurements, to provide secure clock synchronization without shared phase reference. We showed that the setup provides sub-shot-noise scaling in the precision of the desynchronization estimate and is only limited by the photon duration. We determined that our setup provides the precision of the order of a tenth of a picosecond for practical single-photon sources producing telecom frequency photons. We also established the security of the clock synchronization scheme by showing that it fulfills both the requirements of protection against channel delay and man-in-the-middle attacks.

In chapter 4, we considered the clock synchronization at a network level in the presence of dishonest and faulty parties. Again, our proposed counterfactual network consensus setup is resilient against shared phase reference. Furthermore, we showed that the proposed scheme is secure against all adversarial attack models— including intercept-and-resent, man-in-the-middle, Trojan horse, and entangle-and-measure attacks.

In chapter 5, we developed a modified noise-robust setup that made our counterfactual setups resilient to noise and more practical with NISQ-era devices. We then utilize this modified setup for the counterfactual network consensus and compare its practicality to its contemporary quantum consensus algorithms in Chapter 6. For this, we developed a framework using a discrete even quantum network simulator, NetSquid, and used the three performance measures: security, scalability, and decentralization. Using the results in chapters 4 and 5, we showed that the counterfactual setup outperforms its peers in terms of security and scalability. Hence, making it a possible candidate for the future generation of intra-enterprise consortium blockchain consensus.

Some possible future works are as follows:

- Here, we provided a counterfactual clock synchronization protocol that can theoretically achieve the precision of 10^{-13} seconds with current single-photon sources. In the future, it will be interesting to see what precision we can achieve for practical

photonic communication.

- We evaluate the effect of quantum noise on counterfactual synchronization and consensus setups in chapter 5. An interesting future direction would be utilizing a photonic quantum network to test the practical setups.

- Some consortium blockchains like Hyperledger fabric aim to bring Byzantine fault tolerance into their framework. It would be interesting if we could integrate the counterfactual Byzantine agreement (in Chapter 4) into a classical blockchain. In this case, only the consensus or validation part will be counterfactual using NISQ networks.

- Our counterfactual setups utilize photonic systems. With 6G mobile communication utilizing the terahertz frequency range, one interesting area would be considering the performance with optical-terahertz converters for possible integration of our counterfactual clock synchronization for 6G networks.

Bibliography

[1] "IBM Quantum," https://www.ibm.com/blogs/research/2016/05/quantum-computing-time-build-quantum-community/, May 2016.

[2] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug. 2018.

[3] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets," *Nature*, vol. 549, no. 7671, pp. 242–246, Sep. 2017.

[4] J. Zhang, G. Pagano, P. W. Hess, A. Kyprianidis, P. Becker, H. Kaplan, A. V. Gorshkov, Z.-X. Gong, and C. Monroe, "Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator," *Nature*, vol. 551, no. 7682, pp. 601–604, Nov. 2017.

[5] H. Bernien, S. Schwartz, A. Keesling, H. Levine, A. Omran, H. Pichler, S. Choi, A. S. Zibrov, M. Endres, M. Greine *et al.*, "Probing many-body dynamics on a 51-atom quantum simulator," *Nature*, vol. 551, no. 7682, pp. 579–584, Nov. 2017.

[6] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," *Phys. Rev. Lett.*, vol. 73, pp. 58–61, Jul. 1994.

[7] A. D. Ludlow, M. M. Boyd, E. P. J. Ye, and P. O. Schmidt, "Optical atomic clocks," *Rev. Mod. Phys.*, vol. 87, pp. 637–701, Jun. 2015.

[8] N. Huntemannand, C. Sanner, B. Lipphardt, C. Tamm, and E. Peik, "Single-ion atomic clock with 3×10^{-18} systematic uncertainty," *Phys. Rev. Lett.*, vol. 116, p. 063001, Feb. 2016.

[9] F. Riehle, "Optical clock networks," *Nature Photonics*, vol. 11, pp. 25–31, Jan. 2017.

[10] J. Zhang, G. L. Long, Z. Deng, W. Liu, and Z. Lu, "Nuclear magnetic resonance implementation of a quantum clock synchronization algorithm," *Phys. Rev. A*, vol. 70, p. 062322, Dec. 2004.

[11] X.-S. Liu, G.-L. Long, and D.-M. Tong, "Simultaneous space and time synchronization using shared entangled qubits," *Commun. Theor. Phys.*, vol. 40, no. 01, p. 45, Jul. 2003.

[12] V. Ameri, M. Eghbali-Arani, and M. Rafiee, "Synchronization of a periodic modulation of mirrors in an optomechanical system," *Quantum Inf. Process.*, vol. 18, no. 11, p. 349, Oct. 2019.

[13] Y. Yang, J. Jing, and Z. Zhao, "Enhancing estimation precision of parameter for a two-level atom with circular motion," *Quantum Inf. Process.*, vol. 18, no. 4, p. 120, Mar. 2019.

[14] R. He, J.-G. Ma, and J. Wu, "A quantum secure direct communication protocol using entangled beam pairs," *Europhys. Lett.*, vol. 127, no. 5, p. 50006, Oct. 2019.

[15] X. Kong, T. Xin, S.-J. Wei, B. Wang, Y. Wang, K. Li, and G.-L. Long, "Demonstration of multiparty quantum clock synchronization," *Quantum Inf. Process.*, vol. 17, no. 11, p. 297, Sep. 2018.

[16] Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device–independent quantum secure direct communication," *Europhys. Lett.*, vol. 125, no. 4, p. 40004, Mar. 2019.

[17] A. Einstein, "Zur elektrodynamik bewegter körper," *Ann. der Phys.*, vol. 17, no. 1, pp. 891–921, 1905.

[18] J. Borregaard and A. S. Sørensen, "Efficient atomic clocks operated with several atomic ensembles," *Phys. Rev. Lett.*, vol. 111, p. 090802, Aug. 2013.

[19] A. A. Masoudi, S. Dorscher, S. Hafner, U. Sterr, and C. Lisdat, "Noise and instability of an optical lattice clock," *Phys. Rev. A*, vol. 92, p. 063814, Dec. 2015.

[20] H. M. Wiseman, "Defending continuous variable teleportation: why a laser is a clock, not a quantum channel," *J. Opt. B: Quantum Semiclass. Opt.*, vol. 6, no. 8, p. S849, Jul. 2004.

[21] A. Andre, A. Sorensen, and M. Lukin, "Stability of atomic clocks based on entangled atoms," *Phys. Rev. Lett.*, vol. 92, no. 23, p. 230801, 2004.

[22] A. Louchet-Chauvet, J. Appel, J. J. Renema, D. Oblak, N. Kjaergaard, and E. S. Polzik, "Entanglement-assisted atomic clock beyond the projection noise limit," *New J. Phys.*, vol. 12, no. 6, p. 065032, 2010.

[23] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sorensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," *Nat. Photon.*, vol. 10, no. 8, pp. 582–587, Jun. 2014.

[24] M. A. Ullah, J. ur Rehman, and H. Shin, "Quantum frequency synchronization of distant clock oscillators," *Quantum Inf. Process.*, vol. 19, no. 5, p. 144, May 2020.

[25] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced positioning and clock synchronization," *Nature*, vol. 412, no. 6845, p. 417–419, 2001.

[26] V. Giovannetti, S. Lloyd, L. Maccone, and F. Wong, "Clock synchronization with dispersion cancellation," *Phys. Rev. Lett.*, vol. 87, no. 11, p. 117902, 2001.

[27] I. L. Chuang, "Quantum algorithm for distributed clock synchronization," *Phys. Rev. Lett.*, vol. 85, no. 9, p. 2006, Aug. 2000.

[28] M. de Burgh and S. D. Bartlett, "Quantum methods for clock synchronization: Beating the standard quantum limit without entanglement," *Phys. Rev. A*, vol. 72, no. 4, p. 042301, 2005.

[29] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum clock synchronization based on shared prior entanglement," *Phys. Rev. Lett.*, vol. 85, pp. 2010–2013, Aug 2000.

[30] J. Preskill, "Quantum clock synchronization and quantum error correction," *arXiv:quant-ph/0010098*, 2000. [Online]. Available: https://arxiv.org/abs/quant-ph/0010098

[31] U. Yurtsever and J. P. Dowling, "Lorentz-invariant look at quantum clock-synchronization protocols based on distributed entanglement," *Phys. Rev. A*, vol. 65, p. 052317, May 2002.

[32] E. O. Ilo-Okeke, L. Tessler, J. P. Dowling, and T. Byrnes, "Remote quantum clock synchronization without synchronized clocks," *npj Quantum Inf.*, vol. 4, no. 1, p. 40, Aug. 2018.

[33] L. Li, P. Shi, X. Fu, P. Chen, T. Zhong, and J. Kong, "Three-dimensional tradeoffs for consensus algorithms: A review, Early Access," *IEEE Trans. Netw. Serv. Manag*, 2022.

[34] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *J. ACM*, vol. 27, pp. 228–234, 1980.

[35] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, p. 382–401, Jul. 1982.

[36] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology," *Nat. Photon.*, vol. 5, no. 4, pp. 222–229, Apr 2011.

[37] M. Fitzi, N. Gisin, and U. Maurer, "Quantum solution to the Byzantine agreement problem," *Phys. Rev. Lett.*, vol. 87, p. 217901, Nov. 2001.

[38] A. Cabello, "n-particle n-level singlet states: Some properties and applications," *Phys. Rev. Lett.*, vol. 89, p. 100402, Aug. 2002.

[39] S. Iblisdir and N. Gisin, "Byzantine agreement with two quantum-key-distribution setups," *Phys. Rev. A*, vol. 70, p. 034306, Sep. 2004.

[40] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter, "Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection," *Phys. Rev. Lett.*, vol. 100, no. 7, p. 070504, Feb. 2008.

[41] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. Oliveira, M. Papendrecht *et al.*, "Netsquid, a discrete-event simulation platform for quantum networks," *Commun. Phys.*, vol. 4, p. 164, 2021.

[42] A. Smirne, J. Kołodyński, S. F. Huelga, and R. Demkowicz-Dobrzański, "Ultimate precision limits for noisy frequency estimation," *Phys. Rev. Lett.*, vol. 116, p. 120801, Mar. 2016.

[43] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, no. 3, pp. 1–39, Jul. 2017.

[44] X. Duan and P. Jin-Ye, "Effects of quantum noise on quantum clock synchronization," *Commun. Theor. Phys.*, vol. 58, no. 2, p. 213, 2012.

[45] E. M. Kessler, P. Kómár, M. Bishof, L. Jiang, A. S. Sorensen, J. Ye, and M. D. Lukin, "Heisenberg-limited atom clocks based on entangled qubits," *Phys. Rev. Lett.*, vol. 112, no. 19, p. 190403, 2014.

[46] H. Nakazato, T. Tanaka, K. Yuasa, G. Florio, and S. Pascazio, "Measurement scheme for purity based on two two-body gates," *Phys. Rev. A*, vol. 85, p. 042316, Apr. 2012.

[47] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge Univ. Press, 2017.

[48] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge Univ. Press, 2010.

[49] Y. Jeong and H. Shin, "Quantum correlation in squeezed generalized amplitude damping channels with memory," *Sci. Rep.*, vol. 9, no. 1, p. 4035, Mar. 2019.

[50] J. W. Z. Tian, J. Jing, and H. Fan, "Influence of relativistic effects on satellite-based clock synchronization," *Phys. Rev. D*, vol. 93, no. 6, p. 65008, Mar. 2016.

[51] L. Schwarz and S. J. van Enk, "Detecting the drift of quantum sources: Not the de Finetti theorem," *Phys. Rev. Lett.*, vol. 106, p. 180501, May 2011.

[52] H. Salih, Z. H. Li, M. Al-Amri, and M. S. Zubairy, "Protocol for direct counterfactual quantum communication," *Phys. Rev. Lett.*, vol. 110, no. 17, pp. 1–5, Apr. 2013.

[53] J. Liu, X.-X. Jing, and X. Wang, "Quantum metrology with unitary parametrization processes," *Sci. Rep.*, vol. 5, p. 8565, Feb. 2015.

[54] S. Pang and T. A. Brun, "Quantum metrology for a general hamiltonian parameter," *Phys. Rev. A*, vol. 90, p. 022117, Aug. 2014.

[55] R. D. Yates and J. G. David, *Probability And Stochastic Processes*, 2nd ed. John Willey & Sons, 1999.

[56] A. S. Eddington, *The Mathematical Theory of Relativity.* Cambridge Univ. Press, 1924.

[57] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, vol. 76, no. 5, pp. 722–725, 1996.

[58] L. Narula and T. E. Humphreys, "Requirements for secure clock synchronization," *IEEE J. Sel. Top. Signal Process.*, vol. 12, no. 4, pp. 749–762, May 2018.

[59] H. Dai, Q. Shen, C.-Z. Wang, S.-L. Li, W.-Y. Liu, W.-Q. Cai, S.-K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen, Q. Zhang, F. Xu, C.-Z. Peng, and J.-W. Pan, "Towards satellite-based quantum-secure time transfer," *Nat. Photon.*, vol. 16, no. 8, pp. 848–852, Aug. 2020.

[60] Y. Aharonov, E. Cohen, and S. Popescu, "A dynamical quantum Cheshire cat effect and implications for counterfactual communication," *Nat. Commun.*, vol. 12, no. 1, p. 4770, Aug. 2021.

[61] I. Alonso Calafell, T. Strömberg, D. R. M. Arvidsson-Shukur, L. A. Rozema, V. Saggio, C. Greganti, N. C. Harris, M. Prabhu, J. Carolan, M. Hochberg, T. Baehr-Jones, D. Englund, C. H. W. Barnes, and P. Walther, "Trace-free counterfactual communication with a nanophotonic processor," *npj Quantum Inf.*, vol. 5, no. 1, p. 61, Jul. 2019.

[62] T.-G. Noh, "Counterfactual quantum cryptography," *Phys. Rev. Lett.*, vol. 103, no. 23, p. 230501, Dec. 2009.

[63] Z.-H. Li, M. Al-Amri, X.-H. Yang, and M. S. Zubairy, "Counterfactual exchange of unknown quantum states," *Phys. Rev. A*, vol. 100, no. 2, p. 022110, Aug. 2019.

[64] Y. Aharonov and L. Vaidman, "Modification of counterfactual communication protocols that eliminates weak particle traces," *Phys. Rev. A*, vol. 99, no. 1, p. 010103, Jan. 2019.

[65] Y. Cao, Y.-H. Li, Z. Cao, J. Yin, Y.-A. Chen, H.-L. Yin, T.-Y. Chen, X. Ma, C.-Z. Peng, and J.-W. Pan, "Direct counterfactual communication via quantum zeno effect," *Proc. Natl. Acad. Sci.*, vol. 114, no. 19, pp. 4920–4924, May 2017.

[66] Q. Guo, S. Zhai, L.-Y. Cheng, H.-F. Wang, and S. Zhang, "Counterfactual quantum cloning without transmitting any physical particles," *Phys. Rev. A*, vol. 96, no. 5, p. 052335, Nov. 2017.

[67] X. Yang, K. Wei, H. Ma, S. Sun, Y. Du, and L. Wu, "Trojan horse attacks on counterfactual quantum key distribution," *Phys. Lett. A*, vol. 380, no. 18-19, pp. 1589–1592, Apr. 2016.

[68] Z.-H. Li, M. Al-Amri, and M. S. Zubairy, "Direct counterfactual transmission of a quantum state," *Phys. Rev. A*, vol. 92, no. 5, p. 052315, Nov. 2015.

[69] H. Salih, "Tripartite counterfactual quantum cryptography," *Phys. Rev. A*, vol. 90, no. 1, p. 012333, Jul. 2014.

[70] L. Wang, Z.-H. Li, J. Xu, Y. Yang, M. Al-Amri, and M. S. Zubairy, "Exchange unknown quantum states with almost invisible photons," *Opt. Express*, vol. 27, no. 15, pp. 20 525–20 540, Jul. 2019.

[71] H. Salih, "Protocol for counterfactually transporting an unknown qubit," *arXiv:1404.2200 [quant-ph]*, 2014. [Online]. Available: https://arxiv.org/abs/1404.2200

[72] H. Salih, J. R. Hance, W. McCutcheon, T. Rudolph, and J. Rarity, "Deterministic teleportation and universal computation without particle exchange," *arXiv:2009.05564 [quant-ph]*, 2020. [Online]. Available: https://arxiv.org/abs/2009.05564

[73] F. Zaman, Y. Jeong, and H. Shin, "Dual quantum zeno supderdense coding," *Sci. Rep.*, vol. 9, no. 11193, Aug. 2019.

[74] Y. Chen, D. Jian, X. Gu, L. Xie, and L. Chen, "Counterfactual entanglement distribution using quantum dot spins," *J. Opt. Soc. Am. B-Opt. Phys.*, vol. 33, no. 4, pp. 663–669, Jan. 2016.

[75] F. Zaman, Y. Jeong, and H. Shin, "Counterfactual Bell-state analysis," *Sci. Rep.*, vol. 8, no. 1, p. 14641, Oct. 2018.

[76] F. Zaman, H. Shin, and M. Z. Win, "Counterfactual full-duplex communication," *arXiv:1910.03200 [quant-ph]*, 2019. [Online]. Available: https://arxiv.org/abs/1910.03200

[77] F. Zaman, K. Lee, and H. Shin, "Information carrier and resource optimization of counterfactual quantum communication," *Quantum Inf. Process.*, vol. 20, no. 168, May 2021.

[78] F. Zaman, E.-K. Hong, and H. Shin, "Local distinguishability of bell-type states," *Quantum Inf. Process.*, vol. 20, no. 174, May 2021.

[79] R. H. Dicke, "Interaction-free quantum measurements: A paradox," *Am. J. Phys.*, vol. 49, no. 10, pp. 925–930, 1981.

[80] A. Elitzur and L. Vaidman, "Quantum mechanical interaction-free measurement," *Found. Phys.*, vol. 23, no. 76, pp. 987–997, Jul. 1993.

[81] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, "Interaction-free measurement," *Phys. Rev. Lett.*, vol. 74, no. 24, p. 4763, Nov. 1995.

[82] W. M. Itano, D. J. Heinzen, J. J. Bollinger, and D. Wineland, "Quantum Zeno effect," *Phys. Rev. A*, vol. 41, no. 5, p. 2295, Mar. 1990.

[83] T. Petrosky, S. Tasaki, and I. Prigogine, "Quantum Zeno effect," *Phys. Lett. A*, vol. 151, no. 3-4, pp. 109–113, Dec. 1990.

[84] Y. Eldar and A. Oppenheim, "Quantum signal processing," *IEEE Signal Process. Mag.*, vol. 19, no. 6, pp. 12–32, Dec. 2002.

[85] Y. C. Eldar and G. D. Forney, "On quantum detection and the square-root measurement," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 858–872, Mar. 2001.

[86] A. Migdall, S. V. Polyakov, J. Fan, and J. C. Bienfang, *Single-photon generation and detection: physics and applications*. Academic Press, 2013.

[87] E. Meyer-Scott, C. Silberhorn, and A. Migdall, "Single-photon sources: Approaching the ideal through multiplexing," *Rev. Sci. Instrum.*, vol. 91, no. 4, p. 041101, Apr. 2020.

[88] A. B. U'Ren, Y. Jeronimo-Moreno, and H. Garcia-Gracia, "Generation of fourier-transform-limited heralded single photons," *Phys. Rev. A*, vol. 75, p. 023810, Feb. 2007.

[89] Y. Li, T. Xiang, Y. Nie, M. Sang, and X. Chen, "Spectral compression of single-photon-level laser pulse," *Sci. Rep.*, vol. 7, no. 1, p. 43494, Feb. 2017.

[90] V. Krutyanskiy, M. Meraner, J. Schupp, and B. P. Lanyon, "Polarisation-preserving photon frequency conversion from a trapped-ion-compatible wavelength to the telecom c-band," *Appl. Phys. B-Lasers Opt.*, vol. 123, no. 9, p. 228, Aug 2017.

[91] I. Liberal, I. Ederra, and R. W. Ziolkowski, "Designing the bandwidth of single-photon sources with classical antenna techniques," in *2019 13th European Conference on Antennas and Propagation (EuCAP)*, 2019, pp. 1–4.

[92] K. A. G. Fisher, D. G. England, J.-P. W. MacLean, P. J. Bustard, K. J. Resch, and B. J. Sussman, "Frequency and bandwidth conversion of single photons in a room-temperature diamond quantum memory," *Nat. Commun.*, vol. 7, no. 1, p. 11200, Apr. 2016.

[93] V. Averchenko, D. A. Reiß, D. Sych, and G. Leuchs, "Lower bounds for the time-bandwidth product of a single-photon pulse," *Phys. Scr.*, vol. 95, no. 3, p. 034012, Feb. 2020.

[94] M. Krzywinski and N. Altman, "Error bars," *Nat. Methods*, vol. 10, no. 10, pp. 921–922, Oct. 2013.

[95] J. Lee, L. Shen, A. Cerè, J. Troupe, A. Lamas-Linares, and C. Kurtsiefer, "Symmetrical clock synchronization with time-correlated photon pairs," *Appl. Phys. Lett*, vol. 114, no. 10, p. 101102, Mar. 2019.

[96] ——, "Asymmetric delay attack on an entanglement-based bidirectional clock synchronization protocol," *Appl. Phys. Lett*, vol. 115, no. 14, Sep. 2019.

[97] G. Cariolaro, *Quantum Decision Theory: Suboptimization. In: Quantum Communications.* Cham: Springer, 2015, pp. 251–280.

[98] M.-Y. Kao, *Encyclopedia of algorithms.* Springer Science & Business Media, 2016.

[99] A. Acín, "Statistical distinguishability between unitary operations," *Phys. Rev. Lett.*, vol. 87, no. 17, p. 177901, Oct. 2001.

[100] A. Cabello, "Solving the liar detection problem using the four-qubit singlet state," *Phys. Rev. Lett.*, vol. 68, p. 012304, Jul 2003.

[101] R. Rahaman, M. Wieśniak, and M. Żukowski, "Quantum Byzantine agreement via hardy correlations and entanglement swapping," *Phys. Rev. A*, vol. 92, p. 042302, Oct. 2015.

[102] Y. Feng, R. Shi, J. Zhou, and Y. Guo, "Quantum Byzantine agreement with tripartite entangled states," *Int. J. Theor. Phys.*, vol. 58, no. 5, pp. 1482–1498, May 2019.

[103] Q. bin Luo, K. yuan Feng, and M. hui Zheng, "Quantum multi-valued Byzantine agreement based on d-dimensional entangled states," *Int. J. Theor. Phys.*, vol. 58, no. 12, pp. 4025–4032, Sep. 2019.

[104] X. Sun, P. Kulicki, and M. Sopek, "Multi-party quantum Byzantine agreement without entanglement," *Entropy*, vol. 22, no. 10, p. 1152, Oct. 2020.

[105] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, "Experimental quantum multiparty communication protocols," *npj Quantum Inf.*, vol. 2, no. 1, p. 16010, Jun. 2016.

[106] A. Tavakoli, A. Cabello, M. Zukowski, and M. Bourennane, "Quantum clock synchronization with a single qudit," *Sci. Rep.*, vol. 5, no. 1, p. 7982, Jan. 2015.

[107] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, "Reference frames, superselection rules, and quantum information," *Rev. Mod. Phys.*, vol. 79, pp. 555–609, Apr. 2007.

[108] V. Cholvi, "Detectable quantum Byzantine agreement for any arbitrary number of dishonest parties," *arXiv:2112.09437 [quant-ph]*, Dec. 2021.

[109] S. Mishra, K. Thapliyal, A. Parakh, and A. Pathak, "Quantum anonymous veto: A set of new protocols," *arXiv preprint arXiv:2109.06260*, Sep. 2021.

[110] Z.-H. Li, L. Wang, J. Xu, Y. Yang, M. Al-Amri, and M. S. Zubairy, "Counterfactual trojan horse attack," *Phys. Rev. A*, vol. 101, p. 022336, Feb. 2020.

[111] X. Yang, K. Wei, H. Ma, S. Sun, Y. Du, and L. Wu, "Trojan horse attacks on counterfactual quantum key distribution," *Phys. Lett. A*, vol. 380, no. 18, pp. 1589–1592, Apr. 2016.

[112] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, Dec. 1997.

[113] R. Demkowicz-Dobrzański, M. Jarzyna, and J. Kołodyński, "Quantum limits in optical interferometry," *Prog. Opt.*, vol. 60, pp. 345–435, 2015.

[114] C. Liu, J. Liu, J. Zhang, and S. Zhu, "The experimental demonstration of high efficiency interaction-free measurement for quantum counterfactual-like communication," *Sci. Rep.*, vol. 7, no. 1, p. 10875, Sep. 2017.

[115] ——, "Improvement of reliability in multi-interferometer-based counterfactual deterministic communication with dissipation compensation," *Opt. Express*, vol. 26, pp. 2261–2269, Feb. 2018.

[116] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar. 1993.

[117] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

[118] J. ur Rehman and H. Shin, "Entanglement-free parameter estimation of generalized Pauli channels," *Quantum*, vol. 5, p. 490, Jul. 2021.

[119] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, pp. 398–461, 2002.

[120] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, "Experimental quantum multiparty communication protocols," *npj Quantum Inf.*, vol. 2, p. 16010, 2016.

[121] C. H. Chien, T. S. Lin, C. Y. Lu, S. Y. Yuan, and S. Y. Kuo, "Quantum circuit and Byzantine generals problem," in *Proc. 12th IEEE International Conference on Nanotechnology (IEEE-NANO)*, Birmingham, UK, Aug. 2012.

[122] A. Dahlberg, B. van der Vecht, C. D. Donne, M. Skrzypczyk, I. T. Raa, W. Kozlowski, and S. Wehner, "Netqasm—a low-level instruction set architecture for hybrid quantum-classical programs in a quantum internet," *arXiv*, 2021.

[123] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, "Quantum internet protocol stack: A comprehensive survey," *arXiv*, 2022.

[124] C. H. Bennett and G. Brassard, "Quantum cryptography public key distribution and coin tossing." *In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December*, pp. 175–179, 1984.

[125] T. Alexander, N. Kanazawa, D. J. Egger, L. Capelluto, C. J. Wood, A. Javadi-Abhari, and D. C. McKay, "Qiskit pulse programming quantum computers through the cloud with pulses," *Quantum Sci. Technol.*, vol. 5, p. 044006, 2020.

[126] M. A. Ullah and J. W. Setiawan. (2022) Netsquid simulations for quantum consensus algorithms. 2022. Available online: (accessed on 14 March 2022). [Online]. Available: https://github.com/Asadquantum/NetSquidforQBA

List of Publications

- **Journal Papers**

1. Muhammad Asad Ullah, Jason William Setiawan, Junaid ur Rehman, and Hyundong Shin, "On the Robustness of Quantum Algorithms for Blockchain Consensus," *Sensors*, vol. 22, no. 7, article id: 2716, April 2022.
2. Muhammad Asad Ullah, Saw Nang Paing, and Hyundong Shin, "Noise-Robust Quantum Teleportation with Counterfactual Communication," *IEEE Access*, vol. 10, pp. 61484 61493, March 2022.
3. Muhammad Asad Ullah, Junaid ur Rehman, and Hyundong Shin, "Quantum Frequency Synchronization of Distant Clock Oscillators," *Quantum Information Processing*, vol. 19, no. 5, article id: 144, March 2020.
4. Muhammad Asad Ullah, Fakhar Zaman, Junaid ur Rehman, and Hyundong Shin, "Counterfactual Secure Clock Synchronization," *Revised for npj Quantum Information*, March 2022.
5. Muhammad Asad Ullah, Fakhar Zaman, Junaid ur Rehman, and Hyundong Shin, "Secure Counterfactual Byzantine Agreement," *To be Submitted for Publication to Transactions IEEE Transactions on Communications*, 2022.
6. Ahmad Farooq, Muhammad Asad Ullah, Junaid ur Rehman, Kyesan Lee and Hyundong Shin, "Self-Guided Quantum State Learning for Mixed State," *Quantum Information Processing (Accepted for publication)*, June 2022.

7. Junaid ur Rehman, Uman Khalid, Muhammad Asad Ullah, Awais Khan and Hyundong Shin, "NISQ Networking: Functionalities, Challenges, and Applications," *To be Submitted for Publication to IEEE Network*, 2022.
8. Saw Nang Paing, Muhammad Asad Ullah, and Hyundong Shin, "Counterfactual Quantum Phase Estimation Algorithm," *To be Submitted for Publication to Quantum Science and Technology*, 2022.

- **Refereed Conference Proceedings (International)**

1. Muhammad Asad Ullah, Ahmad Farooq, Youngmin Jeong, and Hyundong Shin, "Quantum pulse coding for Rabi and Ramsey evolution on IBM Armonk," in *Proceedings of International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea, October 2021.
2. Muhammad Asad Ullah, Youngmin Jeong, and Hyundong Shin, "Clock synchronization in distributed quantum networks," *in Proceedings of Asian Quantum Information Science (AQIS) Conference*, Nagoya, Japan, September 2018.
3. Muhammad Asad Ullah, Youngmin Jeong, and Hyundong Shin, "Quantum channel switching with optimal fidelity," *in Proceedings of IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, Incheon, Korea, August 2017.

- **Refereed Conference Proceedings (Domestic)**

1. Muhammad Asad Ullah and Hyundong Shin, "Amplitude damping loss in quantum consensus algorithms," *in Proceedings of Korea Information and Communication Society (KICS) Summer Conference*, Jeju, Korea, June 2022.
2. Abdurrahman Wachid Shaffar, Muhammad Asad Ullah, and Hyundong Shin, "Experimental benchmarking between IBM quantum computing systems," *in Proceedings of Korea Information and Communication Society (KICS) Summer Conference*, Jeju, Korea, June 2022.

3. Fadhel Hariz Dzulfikar, Muhammad Asad Ullah, and Hyundong Shin, "Optimal qubits for entangled state creation on IBM quantum Manila device," *in Proceedings of Korea Information and Communication Society (KICS) Summer Conference*, Jeju, Korea, June 2022.

4. Syed Muhammad Abuzar Rizvi, Muhammad Asad Ullah, and Hyundong Shin, "Measurement error mitigation for NISQ devices," *in Proceedings of Korea Information and Communication Society (KICS) Summer Conference*, Jeju, Korea, June 2022.

5. Jason William Setiawan, Muhammad Asad Ullah, and Hyundong Shin, "Fault tolerance of qudit-based private list distribution," *in Proceedings of Korea Information and Communication Society (KICS) Summer Conference*, Jeju, Korea, June 2022.

6. Muhammad Asad Ullah, Jason William Setiawan, Junaid ur Rehman, and Hyundong Shin, "Robustness of entanglement-free quantum Byzantine agreement," *in Proceedings of Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, February 2022.

7. Syed Muhammad Abuzar Rizvi, Muhammad Asad Ullah, and Hyundong Shin, "Machine learning for qubit state estimation on IBM quantum computer," *in Proceedings of Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, February 2022. **[Best Paper Award]**

8. Jason William Setiawan, Muhammad Asad Ullah, Kyesan Lee, and Hyundong Shin, "Throughput analysis of qudit based quantum Byzantine agreement," *in Proceedings of Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, February 2022.

9. Muhammad Asad Ullah, Junaid ur Rehman, and Hyundong Shin, "Photon dynamics in counterfactual quantum communication," *in Proceedings of Korea Information and Communication Society (KICS) Winter Conference*, Pyeongchang, Korea, February 2021.

10. Muhammad Asad Ullah, Junaid ur Rehman, and Hyundong Shin, "On the usefulness of ancilla-assisted entanglement for metrology," *in Proceedings of Korea Information and Communication Society (KICS) Summer Conference*, Pyeongchang, Korea, August

2020.

11. Muhammad Asad Ullah, Youngmin Jeong, and Hyundong Shin, "Accuracy-precision trade-off in quantum phase estimation," *in Proceedings of Joint Conference on Communications and Information (JCCI)*, Gangneung, Korea, May 2019.
12. Muhammad Asad Ullah, Youngmin Jeong, and Hyundong Shin, "Frequency estimation in quantum clock synchronization networks," *in Proceedings of Korea Information and Communication Society (KICS) Fall Conference*, Seoul, Korea, November 2018.
13. Muhammad Asad Ullah, Youngmin Jeong, and Hyundong Shin, "Noisy GHZ states for quantum metrology," *in Proceedings of Korea Information and Communication Society (KICS) Fall Conference*, Daegu, Korea, November 2017.
14. Muhammad Asad Ullah, Youngmin Jeong, and Hyundong Shin, "Hyperentanglement assisted efficient quantum key distribution," *in Proceedings of Korea Information and Communication Society (KICS) Fall Conference*, Seoul, Korea, November 2016.

- **Patents**

1. Hyundong Shin, Muhammad Asad Ullah, and Junaid ur Rehman, "Quantum synchronization method without shared phase reference and quantum communication system thereof," Korea Patent 10-2231135, March 17, 2021. **[Excellent Patent Award]**
2. Hyundong Shin, Muhammad Asad Ullah, Youngmin Jeong, and Fakhar Zaman, "Method of detecting inaccurate slave clocks," Korea Patent 10-2201814, January 06, 2021.
3. Hyundong Shin, Muhammad Asad Ullah, and Youngmin Jeong, "Method of synchronizing quantum network and quantum system performing thereof," Korea Patent 10-2128362, June 24, 2020.
4. Hyundong Shin, Muhammad Asad Ullah, and Youngmin Jeong, "Method of switching quantum channel and system thereof," Korea Patent 10-1984963, May 27, 2019.
5. Hyundong Shin, Muhammad Asad Ullah, and Youngmin Jeong, "System of frequency synchronization, apparatus of frequency synchronization, method of frequency syn-

chronization and method of the same for quantum clock," Korea Patent 10-1953632, February 25, 2019.

6. Hyundong Shin, Muhammad Asad Ullah, and Youngmin Jeong, "Method of synchronization in quantum network,"Korea Patent 10-1945761, January 30, 2019.