Anonymous Communication in Quantum Networks

A dissertation submitted in partial fulfillment for the degree of

Master of Technology

in

Computer Science

by

Anish Majumdar
Roll No. - CS2303

under the supervision of

Dr. Ramij Rahaman
Physics and Applied Mathematics Unit (PAMU)
Indian Statistical Institute, Kolkata

June, 2025

Certificate

This is to certify that the dissertation entitled *"Anonymous Communication in Quantum Networks"* submitted by **Anish Majumdar** to the Indian Statistical Institute, Kolkata, in partial fulfillment of the requirements for the degree of **Master of Technology in Computer Science**, is an authentic and genuine record of the research work carried out by the candidate under my supervision and guidance.

I affirm that the dissertation has met all the necessary requirements in accordance with the regulations of this institute.

Ramij Rahaman. 06/06/25

Ramij Rahaman
Physics and Applied Mathematics Unit (PAMU)
Indian Statistical Institute, Kolkata – 700108, India

Acknowledgement

I extend my sincere appreciation to Dr. Ramij Rahaman, my advisor at the Physics and Applied Mathematic Unit of the Indian Statistical Institute in Kolkata, for his guidance, continuous support, and inspiration. His profound knowledge and creative suggestions have taught me a great deal in every subject and have shown me how to conduct solid research.

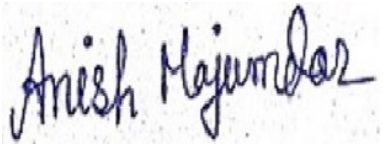
I am deeply grateful to all the teachers at the Indian Statistical Institute for their invaluable advice, insights, and instruction, which provided a crucial perspective to my research.

Finally, I want to express my gratitude to my parents and extended family for their unwavering support. I also extend my sincere appreciation to all my friends for their continuous assistance and encouragement. I am thankful to everyone who has contributed to my growth and success, even if I have inadvertently missed mentioning them in the above list

Declaration

I, **Anish Majumdar**, with Roll No. **CS2303**, hereby declare that the material presented in the dissertation titled *"Anonymous Communication in Quantum Networks"* represents original work carried out by me for the degree of Master of Technology in Computer Science at the Indian Statistical Institute, Kolkata.

Furthermore, I affirm that no sections of this report have been sourced or copied from external references without proper attribution. I am aware that any instances of plagiarism or the use of unacknowledged materials will be treated with the utmost seriousness.



Anish Majumdar
M.Tech (CS), Roll No.- CS2303
Indian Statistical Institute, Kolkata

Abstract

In this dissertation, we explore the protocols enabling anonymous communication in quantum networks i.e. transmission of qubits from sender to receiver by creating or distributing Entangled states between them without disclosing their identities as sender or receiver to the other parties in the network. Existing methods uses classical, as well as quantum sub-protocols to achieve anonymity.The Quantum sub-protocols include protocols for anonymous entanglement distribution using GHZ states, verification (not device-independent) of GHZ state that requires secure private classical channels, techniques for ϵ-anonymity(i.e. the other parties can at most guess a little ϵ amount better than a random guess about who the sender is, due to little impurity in the GHZ state used as a resource).The existing classical sub-protocols also uses secure private classical channels for communication, which is costly to make completely secure. Our contributions include quantum versions of Classical sub-protocols for tasks such as parity(for calculating Boolean-XOR of the input bits of all the parties in the network), logical-OR(for calculating Boolean-OR), Notification done anonymously (i.e. not revealing the input of each party to other parties) without requiring secure private classical channels and device-independent verification (also without requiring secure private classical channels) of GHZ state (of odd number of parties) used as a resource in the sub-protocols. Formal proofs and security analyses demonstrate that our protocols meet the desired anonymity and correctness guarantees. This work lays the groundwork for future anonymous quantum communication systems.

Keywords: Anonymous communication, quantum networks, GHZ state, GHZ verification, Device-independent verification, entanglement, ε-anonymity, teleportation, quantum protocol

Contents

1 Introduction

In a quantum network of a collection of parties or agents, one party (sender) sends quantum bits or qubits (rather than classical bits) to another party (receiver). In this paper our goal is to device a method that keeps the identities of the sender and receiver hidden from the other parties, i.e. keep the sender and receiver anonymous.

The swift advancement of quantum communication networks is poised to enable numerous agents—each with varying levels of classical or quantum technological capability—to securely exchange messages and efficiently collaborate on distributed computational tasks. The examples of initial attempts of distributed computational tasks are the calculation of boolean-XOR (Dining cryptographers problem [1]) and boolean-OR (Anonymous veto [2]) of the input bits of the parties, through classical protocols, anonymously, i.e. keeping the input bit of each party hidden from the other parties. These progresses pave the way for significant innovations in information and communication technologies and is expected to culminate in the realization of a quantum internet [3]. Various applications for quantum networks have already been established, such as quantum key distribution (QKD) [4, 5] and protocols for blind and verifiable delegation of quantum computation [6], with many more potential uses still to be explored.

Among the essential yet complex features that any network must support is the ability to maintain the anonymity of two parties—a Sender and a Receiver—who wish to communicate. In practical settings, it is necessary for this anonymity to be preserved even in the presence of malicious entities. Ideally, such protection should be ensured in an information-theoretic sense, meaning that it must hold without assumptions about the number or computational resources of adversarial agents, including the possibility that they may possess quantum computational power.

In classical contexts, information-theoretic anonymity and secure multiparty computation are achievable when a majority of agents are honest. Notably, Broadbent and Tapp [7] demonstrated that even without an honest majority, anonymous communication of classical messages and other secure tasks can be achieved, provided that secure pairwise classical channels and broadcast mechanisms are available.

In the quantum domain, the pioneering effort to address quantum message anonymity was undertaken by Christandl and Wehner [8]. Their protocol assumes that all n agents share a perfect n-partite GHZ state, specifically $\frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$ [9]. Based on this assumption, they introduced perfectly anonymous protocols for classical bit broadcasting and for establishing

an EPR pair between a Sender and Receiver. These are then combined to enable quantum message transmission through teleportation [10], where an anonymous EPR pair is first established, followed by the anonymous transmission of classical measurement results. This scheme only requires local operations and classical communication (LOCC) once the GHZ state is in place. However, it relies on the assumption that such a GHZ state has been honestly and perfectly distributed among the agents. Later, Lipińska et al. [11] proposed a similar protocol using trusted W states, though only with probabilistic success.

To address the limitation of requiring a perfectly shared quantum state, Brassard et al. [12] proposed a new approach incorporating a verification step that ensures the shared state is symmetric with respect to the honest agents, thus maintaining anonymity. This process involves each agent performing a controlled-NOT operation between their initial qubit and $n-1$ ancillary qubits, which are then distributed to the other agents. After measuring these ancillary qubits in a specific subspace, the protocol proceeds with the remaining GHZ state if the verification passes. While this method achieves perfect anonymity, its implementation is technically demanding, as it necessitates large-scale quantum circuits and full quantum connectivity between agents.

In this work, we tackle the challenge of quantum anonymous transmission under the assumption that the source of the GHZ state cannot be trusted. Our approach combines the Christandl-Wehner protocol for anonymous entanglement [8] with a GHZ state verification protocol described in [13]. We introduce a new concept of *approximate anonymity*, tailored to the practical limitations of real-world quantum networks, and propose a practical, efficient protocol that achieves this form of anonymity in quantum message transmission.

The precise problem statement is as follows. Consider a network with n parties where $k(\leq n)$ parties are honest. Our goal is to construct a protocol to send a quantum message (qubits) from any sender to any receiver such that:

- The identity of the sender remains unknown to all n parties except himself
- The identity of the receiver remains unknown to all except herself and the sender

Our Overall Strategy to do this is as follows. The protocol executes in three phases:

- First, the sender anonymously notifies the receiver,that some message will be sent to the receiver
- Then, with the resource of previously shared n-party GHZ sate, an EPR pair is formed between sender and receiver, in such a way that:

– Probability of guessing by other parties , who the sender is :

$$\Pr[\text{guess sender}] \leq \frac{1}{k} + \epsilon$$

, without the ϵ this would mean random guess amongst the k honest parties,which means full anonymity about the identity of the sender is obtained. That is why with the ϵ it is called ϵ-anonymous.

- Then quantum teleportation is used to send a qubit using that EPR pair.

The remainder of this dissertation is organized into several sections that collectively develop, analyze, and extend protocols for anonymous communication in quantum networks. In Section 2, we introduce the core building blocks of the proposed anonymous communication procedure. This includes a series of classical and quantum sub-protocols such as the Parity Protocol, Logical OR Protocol, and Notification Protocol, all of which enable secure multi-party computation without revealing individual identities. We then proceed to describe the Anonymous Entanglement Protocol, which is crucial for establishing entangled states between anonymous participants. The section also includes rigorous discussions on the correctness and verification of these protocols, particularly focusing on the GHZ state and its extensions to non-GHZ entangled states. Furthermore, we describe an ϵ-anonymous variant of the entanglement distribution protocol and analyze its behavior under noisy conditions.

Section 3 formalizes the anonymity guarantees offered by these protocols. It presents a mathematical framework for evaluating the fidelity of the shared quantum states and culminates in the proof of a key Anonymity Theorem that captures the extent to which sender and receiver identities remain hidden from both honest and dishonest participants.

Section 4 is dedicated to the challenge of verifying the GHZ states in a device-independent setting, where the internal workings of the measurement devices cannot be trusted. We present a detailed analysis of the eigenvalue structure of the relevant observables and construct a device-independent verification scheme based on quantum nonlocal correlations. This is followed by a formal proof of a simultaneous block-diagonalization lemma, which underpins the verification strategy, and an error analysis that quantifies the robustness of the scheme against imperfections.

Section 5 explores the quantum analogues of classical anonymous communication protocols. Here, we examine how the principles and structures of classical protocols can be adapted to quantum settings, preserving their anonymity properties while leveraging the unique advantages of quantum information.

2 Components of the Procedure

The whole procedure or protocol comprises several sub-protocols which are classified into two classes: (i) Anonymous Classical protocols, and (ii) Anonymous Quantum protocols, and are listed below.
(i)Anonymous Classical Protocols:

- Parity
- Logical OR
- Random Bit (anonymous broadcast)
- Notification

(ii)Anonymous Quantum Protocols:

- Anonymous Entanglement
- Verification
- ϵ-Anonymous Entanglement Distribution

I will discuss these sub-protocols one by one in the following sub-sections of this section.

2.1 Parity Protocol

In Parity protocol our goal is to calculate the XOR of the input bits x_i of agent-i in such a way that, everyone's input remain hidden from other agents, i.e. anonymously.

Protocol 1 (Parity Protocol)**.** *Parity*

Input: $\{x_i\}_{i=1}^n$
Goal: *Each agent gets* $y = \bigoplus_{i=1}^n x_i$

1.	*Each agent i chooses random bits $\{r_i^j\}_{j=1}^n$ where $\bigoplus_{j=1}^n r_i^j = x_i$*
2.	*Agent i sends r_i^j to agent j (including themselves), using a secure private channel*
3.	*Each agent j computes $z_j = \bigoplus_{i=1}^n r_i^j$ and broadcasts it*
4.	*The value $z = \bigoplus_{j=1}^n z_j$ calculated by each party equals y*

2.2 Logical OR Protocol

In Logical OR protocol our goal is to calculate the OR of the input bits x_i of agent-i in such a way that, everyone's input remain hidden from other agents, i.e. anonymously.

Protocol 2 (Logical OR Protocol)**.** *LogicalOR*

Input: $\{x_i\}_{i=1}^n$, *security parameter* S
Goal: *Each agent gets* $y_i = \bigvee_{i=1}^n x_i$

---

1. *Agents agree on n orderings with different last participants*

---

2. *For each ordering:*
   a. *Agent i sets:*

$$p_i = \begin{cases} 0 & \text{if } x_i = 0 \\ 1 \text{ or } 0 \text{ with probability } \frac{1}{2} \text{each} & \text{if } x_i = 1 \end{cases}$$

   b. *Run Parity protocol on* $\{p_i\}$*, with a regular broadcast channel rather than simultaneous broadcast, and with the agents broadcasting according to the current ordering.*
   c. *If result is 1, set* $y_i = 1$

---

3. *Repeat S times. If the result is never 1, set* $y_i = 0$

These two protocols requires secure private classical communication channels. Classical cryptography offers channels that are computationally secure. But advent of quantum computers can break such security easily. In that situation security can be achieved by quantum key distribution protocols; but they are costlier. Therefore, I will introduce quantum protocols for calculating Parity and Logical-OR in a latter section, that will not require secure private classical communication channels.

2.3 Analysis of Logical OR Protocol

- If all agents input $x_i = 0$, then Logical OR is correct with probability 1
- If any agent inputs $x_i = 1$, then probability of correctness$= 1 - 2^{-S}$

Proof: Suppose $x_i = x_j = 1$ (and the others are 0), then Expected output = 1, and the protocol fails only if for all S rounds:

$$(p_i = p_j = 1) \text{ OR } (p_i = p_j = 0)$$

, but there are 4 possible combinations of the values of (p_i, p_j). Thus failure probability:

$$= \left(\frac{2}{4}\right)^S = \left(\frac{1}{2}\right)^S$$

2.4 Random Bit Protocol

Protocol 3 (Random Bit Protocol)**.** *RANDOMBIT*

Purpose: *It is used to broadcast any single bit anonymously by any agent*

Input: *all: parameter S. Sender: distribution D*
Goal: *sender chooses a bit according to D*

---

1. *The agents pick bits $\{x_i\}_{i=1}^n$ as follows:*
   - *The sender picks bit (that he wants to broadcast) x_i to be 0 or 1 according to distribution D*
   - *All other agents pick $x_i = 0$*

---

2. *Perform the LOGICAL-OR protocol with input $\{x_i\}_{i=1}^n$ and security parameter S*
   - *Output its outcome*

---

3. ***Properties:***
   - *The outcome of Random Bit is the input of the sender*
   - *If any agent behaves dishonestly, the sender will abort*

2.5 Notification Protocol

Before sending the quantum message or qubits to the intended receiver, the sender notifies her, through this protocol, so that she starts following the steps specific to any receiver.

Protocol 4 (Notification Protocol)**.** *NOTIFICATION*

Input: *security parameter S, sender's choice of receiver r*
Goal: *sender notifies receiver*

1. *For each agent i (i.e. if it is i's turn (to receive)):*
   a. *Each agent $j \neq i$ picks p_j as follows:*
      - *If $i = r$ and agent j is the sender, then:*
        $p_j = 1$ *with probability* $\frac{1}{2}$
        $p_j = 0$ *with probability* $\frac{1}{2}$
      - *Otherwise,* $p_j = 0$
   b. *Let* $p_i = 0$
   c. *Run the PARITY protocol with input* $\{p_i\}_{i=1}^n$*, with modifications:*
      - *Agent i does not broadcast her value*
      - *They use a regular broadcast channel rather than simultaneous broadcast*
      - *If the result is 1, then* $y_i = 1$

2. *Repeat steps 1.(a) - 1.(c) S times:*
   a. *If the result of the PARITY protocol is never 1, then* $y_i = 0$

3. ***Output:*** *If agent i obtained* $y_i = 1$*, then she is the receiver*

When there is no collision i.e. only one sender trying to notify one receiver , this protocol works fine. The cases of collision is addressed in [7]. We also modify this notification protocol to have a fully quantum version in a latter section.The classical protocols end here and we turn to the Quantum protocols next.

2.6 Relevant Quantum Computational Preliminaries

In this section I describe some preliminaries about Quantum computation so that it becomes easy to follow the Anonymous Quantum Protocols in the next sections. In quantum information theory, a fundamental concept is that of **entanglement**, which refers to non-classical correlations between quantum systems that cannot be explained by classical physics. Let us consider two quantum systems A and B, associated with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. A pure state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called a **product state** (or **separable state**) if it can be written as $|\psi\rangle_{AB} = |\psi_A\rangle \otimes |\psi_B\rangle$, where $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$. In contrast, a state is said to be **entangled** if it cannot be expressed in this product form. Entangled states exhibit correlations between the subsystems that do not arise from classical joint distributions and play a crucial role in many quantum protocols.

A prominent class of entangled states are the **EPR pairs**, named after Einstein, Podolsky, and Rosen, who first discussed such correlations in their 1935 paper questioning the completeness of quantum mechanics. The four canonical EPR pairs are often referred to as

the **Bell states**, and are defined for two-qubit systems as follows:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

These states are mutually orthonormal and form a complete basis for the two-qubit Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. Each of them is maximally entangled, meaning that they exhibit the highest possible degree of entanglement for a pair of qubits.

For multipartite systems, a generalization of entanglement is provided by the **GHZ state**, named after Greenberger, Horne, and Zeilinger. The n-qubit GHZ state is given by

$$|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}),$$

which for $n = 3$ takes the form $|\mathrm{GHZ}_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. GHZ states are examples of genuine multipartite entanglement, as the entanglement spans all participating qubits in a way that cannot be reduced to entanglement between pairs or subsets of the system.

A state is said to be **maximally entangled** if, when we consider one part of the system in isolation (by taking the partial trace over the other part), the resulting reduced density matrix is a maximally mixed state. Formally, for a bipartite state $|\psi\rangle_{AB} \in \mathbb{C}^d \otimes \mathbb{C}^d$, if $\mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \frac{1}{d}\mathbb{I}_d$, then the state is maximally entangled. The EPR pairs are maximally entangled with respect to the two-qubit bipartition, while the GHZ state is maximally entangled in a multipartite sense, distributing its entanglement globally across all participating qubits.

These entangled states form the foundation of many essential quantum communication and computation protocols, including quantum teleportation, superdense coding, entanglement-based quantum key distribution, and distributed quantum computation.

The GHZ state famous for the GHZ paradox presents a more direct and striking contradiction between the predictions of quantum mechanics and the assumptions of local realism, without the need for statistical inequalities as in Bell's theorem. It demonstrates that, under certain conditions, quantum mechanics leads to deterministic predictions that are incompatible with any local hidden variable theory.

Consider three spatially separated qubits shared among three parties—Alice, Bob, and

Charlie—prepared in the GHZ state:

$$|\mathrm{GHZ}_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

Let each party choose to measure either the Pauli X or Pauli Y observable on their respective qubit. The paradox arises from examining the correlations between these measurements.

Let us denote the observables by:

- X_i: Pauli X measured by party i
- Y_i: Pauli Y measured by party i

Quantum mechanically, it can be shown that the GHZ state satisfies the following eigenvalue equations:

$$X_1X_2X_3\,|\mathrm{GHZ}_3\rangle = +\,|\mathrm{GHZ}_3\rangle\,,$$

$$X_1Y_2Y_3\,|\mathrm{GHZ}_3\rangle = -\,|\mathrm{GHZ}_3\rangle\,,$$

$$Y_1X_2Y_3\,|\mathrm{GHZ}_3\rangle = -\,|\mathrm{GHZ}_3\rangle\,,$$

$$Y_1Y_2X_3\,|\mathrm{GHZ}_3\rangle = -\,|\mathrm{GHZ}_3\rangle\,.$$

Each of these equations implies that the product of measurement outcomes for the indicated observables must equal the corresponding eigenvalue (either $+1$ or -1) with certainty.

Now, assume that each measurement outcome is predetermined by hidden variables and does not depend on the choice of measurement at other locations (local realism). Then each observable (e.g., X_1, Y_2) must have a definite value ± 1, independent of the measurement context.

Let us assign such predetermined values: $x_i = \pm 1$ for X_i, and $y_i = \pm 1$ for Y_i, for $i = 1, 2, 3$. Then we should have:

$$x_1x_2x_3 = +1$$
$$x_1y_2y_3 = -1$$
$$y_1x_2y_3 = -1$$
$$y_1y_2x_3 = -1$$

Multiplying the last three equations:

$$(x_1y_2y_3)(y_1x_2y_3)(y_1y_2x_3) = (-1)^3 = -1.$$

Simplifying the left-hand side:

$$x_1x_2x_3(y_1)^2(y_2)^2(y_3)^2 = x_1x_2x_3,$$

since $(y_i)^2 = 1$. Therefore, we get:

$$x_1x_2x_3 = -1.$$

But from the first equation, quantum mechanics predicts:

$$x_1x_2x_3 = +1.$$

This is a contradiction. Hence, the predictions of quantum mechanics (as manifested in the GHZ correlations) cannot be reproduced by any local hidden variable theory.

This paradox reveals a deterministic conflict between quantum theory and classical assumptions, without relying on probabilistic inequalities. The GHZ paradox is considered a strong refutation of local realism and provides a conceptually clear demonstration of the nonlocal nature of quantum mechanics.

2.7 Anonymous Entanglement Protocol

This protocol is used to form an EPR pair between the sender and receiver in such a way that the identity of the sender or receiver remains hidden.

Protocol 5 (Anonymous Entanglement Protocol)**.** *ANONYMOUS ENTANGLEMENT*

Input: *n agents share a GHZ state*
Goal: *EPR pair shared between the sender and the receiver*

1. *Each agent, apart from the sender and receiver:*
   a. *Applies a Hadamard transform to their qubit*
   b. *Measures in the computational basis*
   c. *Broadcasts their outcome* m_j

2. *The sender:*
   a. *Picks a random bit* b
   b. *Broadcasts it*
   c. *Applies a phase flip* σ_z *only when* $b = 1$

3. *The receiver:*
   a. *Picks a random bit* b'
   b. *Broadcasts it*
   c. *Applies a phase flip* σ_z *only when the parity of everyone else's broadcasted bits is 1*

2.8 Correctness of Anonymous Entanglement

The shared state ,after the $n-2$ remaining parties apply the Hadamard transform, becomes:

$$I_A \otimes I_B \otimes H^{\otimes(n-2)} \left(\frac{1}{\sqrt{2}}(|0^{\otimes n}\rangle + |1^{\otimes n}\rangle) \right) = \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in \{0,1\}^{n-2}} (|00\rangle|x\rangle + (-1)^{|x|}|11\rangle|x\rangle)$$

,where $|x|$= XOR of the bits in x.

After measurement (j-th party's outcome be m_j), the sender-receiver state is:

$$\frac{1}{\sqrt{2}}(|00\rangle + (-1)^{|x|}|11\rangle)$$

where $|x| = \bigoplus_{j \in V \setminus \{s,r\}} m_j$, where V=set of all the n parties, and s,r are sender and receiver parties respectively.

After sender's phase flip:

$$\frac{1}{\sqrt{2}}(|00\rangle + (-1)^{|x|\oplus b}|11\rangle)$$

Receiver corrects using $b' = |x| \oplus b$, resulting in perfect EPR pair:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

2.9 Verification Protocol

The success of the Anonymous Entanglement Protocol hinges on the genuineness of the GHZ state used. Therefore we should have a check on the shared state as the source of the shared GHZ state may himself be dishonest.

Protocol 6 (Verification Protocol)**.** *VERIFICATION*

Input: *n agents share state* $|\Psi\rangle$
Goal: *to verify that* $|\Psi\rangle$ *is a GHZ state, where k agents are honest*

---

1. *The verifier:*
   a. *Generates random angles* $\theta_j \in [0, \pi)$ *for all* $j \in [n]$
   b. *Ensures* $\sum_j \theta_j$ *is a multiple of* π
   c. *Distributes angles to all agents via secure private channels*

---

2. *Agent j:*
   a. *Measures in basis* $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\}$ *where:*
   $|\pm_{\theta_j}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\theta_j}|1\rangle)$
   b. *Reports outcome* $Y_j \in \{0, 1\}$ *to verifier via secure private channels*

---

3. *Verification passes if:*
   $\bigoplus_j Y_j = \frac{1}{\pi}\sum_j \theta_j \pmod 2$

This verification procedure of the GHZ state is not device independent (dimension independent), i.e. its correctness depends on the genuineness of the measurement apparatus used in the protocol. In a latter section I will introduce a new device-independent verification procedure for GHZ state.

2.10 GHZ State Verification

The verification protocol provides a method to confirm whether the shared quantum state $|\Psi\rangle$ is a genuine n-partite GHZ state of the form:

$$|G_0^n\rangle = \frac{1}{\sqrt{2}}(|0^{\otimes n}\rangle + |1^{\otimes n}\rangle)$$

When all parties are honest and share a perfect GHZ state, the verification succeeds with probability 1. The process works as follows:

1. **Rotation and Measurement:** Each agent j receives a random angle θ_j and measures their qubit in the basis $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\}$. This measurement is equivalent to first applying

the rotation operator:

$$R_z(\theta_j) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\theta_j} \end{bmatrix}$$

to their qubit and then measuring in the Pauli-X basis $\{|+\rangle, |-\rangle\}$.

2. **State Transformation:** For a true GHZ state, applying these rotations yields:

$$\frac{1}{\sqrt{2}}(|0^{\otimes n}\rangle + e^{-i\theta}|1^{\otimes n}\rangle)$$

where $\theta = \sum_{j=1}^{n} \theta_j$ is the sum of all rotation angles.

3. **Parity Condition:** The verification test is passed if the parity of measurement outcomes matches the phase condition:

$$\bigoplus_{j=1}^{n} Y_j = \frac{1}{\pi} \sum_{j=1}^{n} \theta_j \pmod 2$$

This condition must hold for two cases:

- When $\theta \equiv 0 \pmod{2\pi}$: The state becomes $\frac{1}{\sqrt{2}}(|0^{\otimes n}\rangle + |1^{\otimes n}\rangle)$ which when written in the Pauli X basis is given by a linear summation of terms with even number(out of n parties) of $|-\rangle$ states and yields even parity
- When $\theta \equiv \pi \pmod{2\pi}$: The state becomes $\frac{1}{\sqrt{2}}(|0^{\otimes n}\rangle - |1^{\otimes n}\rangle)$ which when written in the Pauli X basis is given by a linear summation of terms with odd number(out of n parties) of $|-\rangle$ states and yields odd parity

$\therefore$The GHZ state will always pass this verification test i.e. :

$$P(\text{pass}) = 1$$

for any choice of angles $\{\theta_j\}$ satisfying the π-multiple condition. This follows from the intrinsic correlation properties of the GHZ state when measured in appropriately rotated bases.

2.11 Non-GHZ States

For non-GHZ states (ρ), we have the following theorems relating, the the probability $P(\rho)$ of passing the verification test by the non-GHZ state, and, the fidelity $F(\rho|G_0^n)$ between the non-GHZ state and a GHZ state.

Theorem 1 (Honest case)**.** *Let ρ be the state shared between n parties, if $F(\rho|G_0^n) := \langle G_0^n|\rho|G_0^n\rangle$, where $|G_0^n\rangle$ is an n-qubit GHZ-state, then*

$$F(\rho) \geq 2P(\rho) - 1 \quad or \quad P(passing\ test) = P(\rho) \leq \frac{1}{2} + \frac{1}{2}F(\rho).$$

Proof: Let us define a test in order to verify a rotated GHZ-state, namely

$$|G_\Theta^n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + e^{-(i\Theta)} \cdot |1\rangle^{\otimes n}), \quad \text{where } \Theta \in [0, 2\pi].$$

Here, the sum of the angles of the parties has to comply with the condition:

$$\sum_{j=1}^{n} \theta_j - \Theta = 0 \,(\mathrm{mod}\, 2\pi).$$

The test that we are interested in is the following:

$$\bigoplus_{j=1}^{n} Y_j = \frac{\sum_{j=1}^{n} \theta_j - \Theta}{\pi} \,(\mathrm{mod}\, 2),$$

which means verification-test passed.

Let $\{P_\Theta^n, I - P_\Theta^n\}$ be the POVM that corresponds to the above test, where clicking of P_Θ^n as a result of the measurements means the test is passed.

We will prove by induction that:

$$P_\Theta^n = |G_\Theta^n\rangle\langle G_\Theta^n| + \frac{1}{2}I_n^\Theta,$$

where I_n is the projector on the space orthogonal to $|G_\Theta^n\rangle$ and $|G_{\Theta+\pi}^n\rangle$. Hence,

$$I - P_\Theta^n = |G_{\Theta+\pi}^n\rangle\langle G_{\Theta+\pi}^n| + \frac{1}{2}I_n^\Theta$$

For $n = 1$, we have that $P_\Theta^1 = |G_\Theta^1\rangle\langle G_\Theta^1|$, so the statement holds. We assume it is true for n and show the statement is true for $n + 1$.

Let us change the protocol a little for $n+1$. Let the angle sent to the 1st party be always θ_1. Then let, the POVM as a function of θ_1 be

$$\left\{P_\Theta^{n+1}(\theta_1), I - P_\Theta^{n+1}(\theta_1)\right\},$$

but as θ_1 is chosen uniformly at random from the interval $[0, \pi]$, the actual measurement

probabilities , P_Θ^{n+1} is given by,

$$P_\Theta^{n+1} = \frac{1}{\pi}\int_0^\pi d\theta_1\, P_\Theta^{n+1}(\theta_1).$$

There are two cases for the test to pass:

1. Party 1 outputs $Y_i = 0$. Then the following equality should hold:

$$\bigoplus_{j=2}^{n+1} Y_j = \frac{\sum_{j=2}^{n+1}\theta_j - (\Theta - \theta_1)}{\pi} \pmod 2.$$

2. Party 1 outputs $Y_i = 1$. Then,

$$\bigoplus_{j=2}^{n+1} Y_j = \frac{\sum_{j=2}^{n+1}\theta_j - (\Theta - \theta_1 + \pi)}{\pi} \pmod 2.$$

Now suppose $\{\Pi_i\}$ is a POVM. If I knows the probabilities $p_j^i = \langle\psi_j^i|\Pi_i|\psi_j^i\rangle$ on a complete basis $\{|\psi_j\rangle\}$, then I can construct $\Pi_i = \sum_j p_j^i|\psi_j\rangle\langle\psi_j|$.

Just like this, as in case 1, $Y_i = 0$ means Party 1's state collapsed to $|G_{\theta_1}^1\rangle$ and $Y_i = 1$ (case 2) means Party 1's state collapsed to $|G_{\theta_1+\pi}^1\rangle$, so we can construct $P_\Theta^{n+1}(\theta_1)$ from Cases 1 & 2 as:

$$\begin{aligned}
P_\Theta^{n+1}(\theta_1) &= |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1| \otimes P_{\Theta'}^n + |G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1| \otimes (I - P_{\Theta'}^n) \;\; [where, \Theta' = \Theta - \theta_1] \\
&= |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1| \otimes |G_{\Theta'}^n\rangle\langle G_{\Theta'}^n| + |G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1| \otimes |G_{\Theta'+\pi}^n\rangle\langle G_{\Theta'+\pi}^n| \\
&\quad + \frac{1}{2}\left(|G_{\theta_1}^1\rangle\langle G_{\theta_1}^1| + |G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1|\right) \otimes I_n^{\Theta'} \quad [using\ definition\ of\ P_{\Theta'}^n] \\
&= |G_\Theta^{n+1}\rangle\langle G_\Theta^{n+1}| + |\Phi_{\theta_1}\rangle\langle\Phi_{\theta_1}| + \frac{1}{2} I_1 \otimes I_n^{\Theta'}, \qquad (1)
\end{aligned}$$

where we define:

$$|\Phi_\alpha\rangle = \frac{1}{\sqrt{2}}\left(|G_\alpha^1\rangle \cdot |G_{\Theta-\alpha}^n\rangle - |G_{\alpha+\pi}^1\rangle \cdot |G_{\Theta-\alpha+\pi}^n\rangle\right).$$

Now, it is easy to verify that:

$$I_{n+1}^\Theta = |\Phi_{\theta_1}\rangle\langle\Phi_{\theta_1}| + |\Phi_{\theta_1+\frac{\pi}{2}}\rangle\langle\Phi_{\theta_1+\frac{\pi}{2}}| + I_1 \otimes I_n^{\Theta'}, \qquad (2)$$

by writing $I_n^{\Theta'} = I_n - |G_{\Theta'}^n\rangle\langle G_{\Theta'}^n| - |G_{\Theta'+\pi}^n\rangle\langle G_{\Theta'+\pi}^n|$ and writing the GHZ states in Z-basis.

$$\begin{aligned}\therefore P_\Theta^{n+1} &= \frac{1}{\pi}\int_0^\pi P_\Theta^{n+1}(\theta_1)\,d\theta_1 \\ &= \frac{1}{\pi}\int_0^{\pi/2}\left[P_\Theta^{n+1}(\theta_1) + P_\Theta^{n+1}(\theta_1+\frac{\pi}{2})\right]\,d\theta_1 \\ &= |G_\Theta^{n+1}\rangle\langle G_\Theta^{n+1}| + \frac{1}{2}I_{n+1}^\Theta. \quad [using\ eq^n s\ 1,2]\end{aligned}$$

Therefore, as a special case $\Theta = 0 (\mathrm{mod}\, 2\pi)$ we can easily see the verification test is just the POVM measurement $\{P_0^n, I - P_0^n\}$.

Now we can express a state ρ with fidelity $F(\rho)$ with GHZ state as,

$$\rho = F(\rho)|G_0^n\rangle\langle G_0^n| + (1 - F(\rho))\chi,$$

where, χ is a $2^n \times 2^n$ density with zero in place of $|G_0^n\rangle\langle G_0^n|$.

$$\therefore P(\rho) = \mathrm{Tr}(P_0^n\rho) = \mathrm{Tr}\left(\left\{\ |G_0^n\rangle\langle G_0^n| + \frac{1}{2}I_n^o\ \right\}\{\ F(\rho)|G_0^n\rangle\langle G_0^n| + (1-F(\rho))\chi\ \}\right)$$

$$= \mathrm{Tr}\left(F(\rho)|G_0^n\rangle\langle G_0^n|\right) + (1-F(\rho))\langle G_0^n|\chi|G_0^n\rangle + \frac{1}{2}F(\rho)\langle G_0^n|I_n^o|G_0^n\rangle + \frac{(1-F(f))}{2}\mathrm{Tr}(I_n^o\chi)$$

$$\leq F(\rho) + 0 + 0 + (\frac{1}{2} - \frac{1}{2}F(\rho)) = \frac{1}{2} + \frac{1}{2}F(\rho).$$

Theorem 2 (Dishonest Case)**.** *Let $\rho = \sum_{r=1}^R p_r|r\rangle\langle r| \otimes \rho_r$ be the state shared between n parties in the space $H_{honest}D_{dishonest}$. If,*

$$F'(\rho) := \sum_r p_r \max_{U_{n-k}^r} F((I_k \otimes U_{n-k}^r)\rho_r(I_k \otimes U_{n-k}^r)^\dagger,\ |G_0^n\rangle),$$

where U_{n-k}^r are operators on the space of the dishonest parities then,

$$F'(\rho) \geq 4P(\rho) - 3 \quad or \quad P(\rho) \leq \frac{3}{4} + \frac{1}{4}F'(\rho).$$

Proof. We proceed by analyzing three progressively general cases: pure states, mixed states without classical information, and fully general mixed states with classical side information.

Case 1: Pure States without Classical Information. Assume that $\rho = |\Psi\rangle\langle\Psi|$, a pure state shared between k honest and $n-k$ dishonest parties.

We decompose $|\Psi\rangle$ using a basis adapted to the honest parties' subspace:

$$|\Psi\rangle = |G_\theta^k\rangle|\Psi_\theta\rangle + |G_{\theta+\pi}^k\rangle|\Psi_{\theta+\pi}\rangle + |\mathcal{X}\rangle,$$

where:

- $\theta = \sum_{j\in H}\theta_j \mod \pi$ is the collective "honest angle",
- $|G_\alpha^k\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + e^{i\alpha}|1\rangle^{\otimes k})$,
- The vector $|\mathcal{X}\rangle$ has its honest part orthogonal to both $|G_\theta^k\rangle$ and $|G_{\theta+\pi}^k\rangle$.

The dishonest parties aim to distinguish between the two branches $|\Psi_\theta\rangle$ and $|\Psi_{\theta+\pi}\rangle$ by performing the optimal Helstrom measurement, whose success probability is:

$$\Pr[\text{guess } Y_H|\theta] = \frac{1}{2} + \frac{1}{2}\left\||\Psi_\theta\rangle\langle\Psi_\theta| - |\Psi_{\theta+\pi}\rangle\langle\Psi_{\theta+\pi}|\right\|_1,$$

where $\|\cdot\|_1$ denotes the trace norm.

The trace norm for rank-2 projectors can be evaluated explicitly:

$$\left\||\Psi_\theta\rangle\langle\Psi_\theta| - |\Psi_{\theta+\pi}\rangle\langle\Psi_{\theta+\pi}|\right\|_1 = \sqrt{\left(\|\Psi_\theta\|^2 + \|\Psi_{\theta+\pi}\|^2\right)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2}.$$

Thus,

$$\Pr[\text{guess } Y_H|\theta] = \frac{1}{2} + \frac{1}{2}\sqrt{\left(\|\Psi_\theta\|^2 + \|\Psi_{\theta+\pi}\|^2\right)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2}.$$

Let us denote $p_\theta := \|\Psi_\theta\|^2$, $q_\theta := \|\Psi_{\theta+\pi}\|^2$. Then we can write:

$$\Pr[\text{guess } Y_H|\theta] \le \frac{3}{4} + \frac{1}{4}\left((p_\theta + q_\theta)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2\right). \tag{3}$$

We now analyze the inner product $\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle$. Consider the Schmidt decomposition:

$$|G_\theta^k\rangle|\Psi_\theta\rangle + |G_{\theta+\pi}^k\rangle|\Psi_{\theta+\pi}\rangle = |A_0\rangle|B_0\rangle + |A_1\rangle|B_1\rangle,$$

where $\langle A_0|A_1\rangle = 0$, $\langle B_0|B_1\rangle = 0$, and:

$$\||B_0\rangle\|^2 = p_\theta, \quad \||B_1\rangle\|^2 = q_\theta.$$

Since the subspace spanned by $|A_0\rangle$, $|A_1\rangle$ is also spanned by $|G_\theta^k\rangle$, $|G_{\theta+\pi}^k\rangle$, we can write:

$$|A_0\rangle = z_0|G_\theta^k\rangle + z_1|G_{\theta+\pi}^k\rangle, \quad |A_1\rangle = z_1^*|G_\theta^k\rangle - z_0^*|G_{\theta+\pi}^k\rangle,$$

with $|z_0|^2 + |z_1|^2 = 1$. Then:

$$|\Psi_\theta\rangle = z_0|B_0\rangle + z_1^*|B_1\rangle, \quad |\Psi_{\theta+\pi}\rangle = z_1|B_0\rangle - z_0^*|B_1\rangle.$$

The overlap becomes:

$$\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle = (p_\theta - q_\theta)z_0 z_1,$$

and thus:

$$|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2 = (p_\theta - q_\theta)^2|z_0|^2|z_1|^2.$$

Now, as $|z_0|^2|z_1|^2 \leq \frac{1}{4}$ (since it's maximized when $|z_0| = |z_1| = \frac{1}{\sqrt{2}}$), we get:

$$|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2 \leq \frac{1}{4}(p_\theta - q_\theta)^2.$$

Substituting into Eq. (3):

$$\Pr[\text{guess } Y_H|\theta] \leq \frac{3}{4} + \frac{1}{4}\left((p_\theta + q_\theta)^2 - (p_\theta - q_\theta)^2\right) = \frac{3}{4} + p_\theta q_\theta.$$

Now, we compute the fidelity with the ideal GHZ state $|G_0^n\rangle$. Since the honest reduced state of $|\Psi\rangle$ is:

$$\rho_H = p_\theta|A_0\rangle\langle A_0| + q_\theta|A_1\rangle\langle A_1| + (\text{noise}),$$

and the honest marginal of $|G_0^n\rangle$ is:

$$\sigma_H = \frac{1}{2}(|A_0\rangle\langle A_0| + |A_1\rangle\langle A_1|),$$

we can bound the fidelity as:

$$F'(\rho) = \left(\text{Tr}\left[\sqrt{\sqrt{\rho_H}\sigma_H\sqrt{\rho_H}}\right]\right)^2 \geq (p_\theta + q_\theta)^2 - \frac{(p_\theta - q_\theta)^2}{2}.$$

Rewriting the previous bound on guessing probability:

$$P(\rho) = \frac{1}{\pi}\int_0^\pi \Pr[\text{guess } Y_H|\theta]d\theta \leq \frac{3}{4} + \frac{1}{4}F'(\rho).$$

Case 2: Mixed State without Classical Information.

Let $\rho = \sum_j q_j|\Psi_j\rangle\langle\Psi_j|$. Since both $F'(\cdot)$ and $P(\cdot)$ are linear in mixtures, we have:

$$P(\rho) = \sum_j q_j P(|\Psi_j\rangle\langle\Psi_j|) \leq \frac{3}{4} + \frac{1}{4}\sum_j q_j F'(|\Psi_j\rangle\langle\Psi_j|) = \frac{3}{4} + \frac{1}{4}F'(\rho).$$

Case 3: General Case with Classical Information.

For $\rho = \sum_r p_r |r\rangle\langle r| \otimes \rho_r$, by applying the previous case on each ρ_r, we get:

$$\begin{aligned} P(\rho) &= \sum_r p_r P(\rho_r) \leq \sum_r p_r \left(\frac{3}{4} + \frac{1}{4} F'(\rho_r) \right) \\ &= \frac{3}{4} + \frac{1}{4} \sum_r p_r \max_{U^r_{n-k}} F\left((I_k \otimes U^r_{n-k}) \rho_r (I_k \otimes U^r_{n-k})^\dagger, |G^n_0\rangle \right) = \frac{3}{4} + \frac{1}{4} F'(\rho). \end{aligned}$$

□

2.12 ϵ-Anonymous Entanglement Distribution Protocol

This is the main protocol that will run and call the previous protocols as subroutines inside it.

Protocol 7 (ϵ-Anonymous Protocol)**.** *ϵ-ANONYMOUS ENTANGLEMENT DISTRIBUTION*

Input: *security parameter S*

Goal: *EPR pair created between sender and receiver with ϵ-anonymity*

1. ***Notification:*** *The sender notifies the receiver.Agents Run Notification protocol.*
2. ***GHZ state generation:*** *Source generates and distributes n-party state $|\Psi\rangle$*
3. ***"Verification" or "Anonymous Entanglement" choice made by sender:***
   a. *The agents perform RandomBit protocol.Sender chooses his input according to the following probability distribution: he flips S fair classical coins, and if all coins are heads, he inputs 0, else he inputs 1. Let the outcome be x*
   b. *If outcome $x = 0$:*
      i. *The agents run Anonymous Entanglement*
   c. *If $x = 1$:*
      i. *Run RandomAgent protocol (i.e. run RandomBit $\log_2 n$ times) , where the sender inputs a uniformly random $j \in [n]$, to get output j (binary of j is at most $\log_2 n$ bits long)*
      ii. *Agent j runs Verification protocol as the verifier*
      iii. *If accepted, return to step 2*
      iv. *Else abort*

2.13 Analysis of ϵ-Anonymous Protocol

Theorem 3. *Let C_ϵ denote the event that the ϵ-Anonymous Entanglement Distribution Protocol does not abort. Suppose the shared state ρ has fidelity:*

$$F'(\rho) = \max_U F(U_{n-k}\rho U_{n-k}^\dagger, |G_0^n\rangle) \leq \sqrt{1-\epsilon^2}$$

Then the probability that the protocol does not abort is bounded by:

$$\Pr[C_\epsilon] \leq 2^{-S} \cdot \frac{4n}{1-\sqrt{1-\epsilon^2}}$$

Proof:

Each round of the protocol consists of the sender deciding whether to proceed with anonymous entanglement or run a verification test. This is decided via the RandomBit protocol with S coin flips.

- With probability 2^{-S}, the sender inputs 0, and anonymous entanglement is performed.
- With probability $1-2^{-S}$, the sender inputs 1.

However, the RandomBit protocol only outputs the correct value with probability $1-2^{-S}$ (due to its probabilistic nature). So the actual probability that verification is correctly triggered is:

$$(1-2^{-S})^2$$

Let us define this as:

$$p_{\text{ver}} = (1-2^{-S})^2$$

Now consider the probability of passing the verification test:

- If the verifier is one of the $n-k$ dishonest agents, they always accept the test (probability 1).
- If the verifier is one of the k honest agents, the test passes with probability at most:

$$P(\rho) \leq \frac{3}{4} + \frac{1}{4}F'(\rho)$$

So the overall probability of passing verification is:

$$P_{\text{pass}} = \frac{n-k}{n} \cdot 1 + \frac{k}{n} \cdot P(\rho) \leq \frac{n-k}{n} + \frac{k}{n}\left(\frac{3}{4} + \frac{1}{4}\sqrt{1-\epsilon^2}\right)$$

Simplifying this:

$$P_{\text{pass}} \leq 1 - \frac{k}{n}\left(1 - \frac{3}{4} - \frac{1}{4}\sqrt{1-\epsilon^2}\right) = 1 - \frac{k}{n} \cdot \frac{1-\sqrt{1-\epsilon^2}}{4}$$

Let us now denote:

$$q := p_{\text{ver}} \cdot P_{\text{pass}} = (1-2^{-S})^2 \cdot \left[\frac{n-k}{n} + \frac{k}{n}\left(\frac{3}{4} + \frac{1}{4}\sqrt{1-\epsilon^2}\right)\right]$$

This q is the probability that a given verification round is chosen and passes.

Let $\Pr[C_\epsilon^\ell]$ be the probability that the protocol proceeds through $\ell - 1$ successful verification rounds, and in round ℓ the sender chooses anonymous entanglement. Then:

$$\Pr[C_\epsilon^\ell] = 2^{-S} \cdot q^{\ell-1}$$

So the total probability of not aborting is:

$$\Pr[C_\epsilon] = \sum_{\ell=1}^{\infty} \Pr[C_\epsilon^\ell] = 2^{-S} \sum_{\ell=0}^{\infty} q^\ell = \frac{2^{-S}}{1-q}$$

To upper-bound this, we observe that $q < 1$ (for any $\epsilon > 0$). To bound the expression $\frac{1}{1-q}$, we begin by expanding q:

$$q = (1-2^{-S})^2 \cdot \left[\frac{n-k}{n} + \frac{k}{n}\left(\frac{3}{4} + \frac{1}{4}\sqrt{1-\epsilon^2}\right)\right]$$

Since $(1-2^{-S})^2 < 1$, we can upper-bound q by ignoring this multiplicative factor:

$$q \leq \frac{n-k}{n} + \frac{k}{n}\left(\frac{3}{4} + \frac{1}{4}\sqrt{1-\epsilon^2}\right)$$

We simplify the right-hand side:

$$\begin{aligned} q &\leq 1 - \frac{k}{n}\left[1 - \left(\frac{3}{4} + \frac{1}{4}\sqrt{1-\epsilon^2}\right)\right] \\ &= 1 - \frac{k}{n} \cdot \left(\frac{1}{4}(1-\sqrt{1-\epsilon^2})\right) \end{aligned}$$

Therefore,

$$1 - q \geq \frac{k}{n} \cdot \frac{1-\sqrt{1-\epsilon^2}}{4} \Rightarrow \frac{1}{1-q} \leq \frac{4n}{k(1-\sqrt{1-\epsilon^2})}$$

This gives the desired upper bound.

Now, use the inequality:

$$1 - q \geq \frac{k}{n} \cdot \frac{1 - \sqrt{1 - \epsilon^2}}{4} \Rightarrow \frac{1}{1 - q} \leq \frac{4n}{k(1 - \sqrt{1 - \epsilon^2})}$$

Thus:

$$\Pr[C_\epsilon] \leq 2^{-S} \cdot \frac{4n}{k(1 - \sqrt{1 - \epsilon^2})} \leq 2^{-S} \cdot \frac{4n}{(1 - \sqrt{1 - \epsilon^2})}$$

To ensure $\Pr[C_\epsilon] \leq \delta$, we choose:

$$S = \log_2 \left(\frac{4n}{k(1 - \sqrt{1 - \epsilon^2})\delta} \right)$$

Conclusion: The probability that the protocol does not abort is exponentially small in S, and can be made less than any desired δ by setting S appropriately.

3 Anonymity Guarantees

In this section I will show that in the last protocol described in previous section the sender remains anonymous. We require some lemmas for the proof of the main anonymity theorem in subsection 3.2.

3.1 Fidelity Bounds

Lemma 1 (State Transformation Under Sender's Transformation)**.** *For the n-partite GHZ state* $|\Phi_0^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$*, the following transformations hold:*

$$\sigma_z|\Phi_0^n\rangle = |\Phi_1^n\rangle \quad \textit{and} \quad \sigma_z|\Phi_1^n\rangle = |\Phi_0^n\rangle$$

where $|\Phi_1^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle - |1^n\rangle)$*.*

Lemma 2 (Honest Case Fidelity)**.** *If all agents are honest and share a state* $|\Psi\rangle$ *with fidelity* $F(|\Psi\rangle, |\Phi_0^n\rangle) = \sqrt{1 - \epsilon^2}$*, then for any two honest potential senders* i, j*:*

$$F(|\Psi_i\rangle, |\Psi_j\rangle) \geq 1 - \epsilon^2$$

where $|\Psi_i\rangle$ *is the state after agent* i *applies the sender's transformation* σ_z*.*

Proof. The shared state can be decomposed as:

$$|\Psi\rangle = (1-\epsilon^2)^{1/4}|\Phi_0^n\rangle + \epsilon_1|\Phi_1^n\rangle + \sum_{k=2}^{2^n-1}\epsilon_k|\Phi_k^n\rangle$$

with $\sum_{k=1}^{2^n-1}\epsilon_k^2 = 1-\sqrt{1-\epsilon^2}$.

When agent i applies σ_z:

$$|\Psi_i\rangle = (1-\epsilon^2)^{1/4}|\Phi_1^n\rangle + \epsilon_1|\Phi_0^n\rangle + \sum_{k=2}^{2^n-1}\epsilon'_k|\Phi_k^n\rangle$$

Likewise,

$$|\Psi_j\rangle = (1-\epsilon^2)^{1/4}|\Phi_1^n\rangle + \epsilon_1|\Phi_0^n\rangle + \sum_{k=2}^{2^n-1}\epsilon''_k|\Phi_k^n\rangle$$

The fidelity between $|\Psi_i\rangle$ and $|\Psi_j\rangle$ is:

$$\begin{aligned} F(|\Psi_i\rangle, |\Psi_j\rangle) &= \left|\sqrt{1-\epsilon^2} + \epsilon_1^2 + \sum_{k=2}^{2^n-1}\epsilon'_k\epsilon''_k\right|^2 \\ &\geq \left|\sqrt{1-\epsilon^2} + \epsilon_1^2 - \left(1-\sqrt{1-\epsilon^2}\right)\right|^2 \quad \left(\because \sum_{k=1}^{2^n-1}\epsilon'^2_k = \sum_{k=1}^{2^n-1}\epsilon''^2_k = 1-\sqrt{1-\epsilon^2}\right) \\ &\geq 1-2\epsilon^2 \end{aligned}$$

□

Lemma 3 (Dishonest Case Fidelity)**.** *If some agents are malicious and the shared state* $|\Psi\rangle$ *has* $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$*, then for honest potential senders* i, j*:*

$$F(|\Psi_i\rangle, |\Psi_j\rangle) \geq 1-\epsilon^2$$

where F' *is the maximum fidelity achievable by malicious parties applying unitary operations on their qubits.*

Proof. Recall that our fidelity measure is given by $F'(|\Psi\rangle) = \max_U F(U|\Psi\rangle, |\Phi_0^n\rangle)$. Let us now denote by $|\Psi'\rangle = U|\Psi\rangle$ the state after the operation U which maximises this fidelity has been applied. We can write this state in the most general form as:

$$|\Psi'\rangle = |\Phi_0^k\rangle|\psi_0\rangle + |\Phi_1^k\rangle|\psi_1\rangle + |\chi\rangle,$$

where note that $|\chi\rangle$ contains both honest and malicious parts, of which the honest part is

orthogonal to both $|\Phi_0^k\rangle$ and $|\Phi_1^k\rangle$.

We want to find the closeness of the states $|\Psi_i\rangle, |\Psi_j\rangle$, which are the states after the $\sigma_x\sigma_z$ operation is applied to $|\Psi'\rangle$ by either agent i or j who is the Sender. These states are given by:

$$|\Psi_i\rangle = |\Phi_1^k\rangle|\psi_0\rangle - |\Phi_0^k\rangle|\psi_1\rangle + |\chi'\rangle,$$
$$|\Psi_j\rangle = |\Phi_1^k\rangle|\psi_0\rangle - |\Phi_0^k\rangle|\psi_1\rangle + |\chi''\rangle.$$

The fidelity is then given by:

$$F(|\Psi_i\rangle, |\Psi_j\rangle) = |\langle\Psi_i|\Psi_j\rangle|^2 = |\langle\psi_0|\psi_0\rangle + \langle\psi_1|\psi_1\rangle + \langle\chi'|\chi''\rangle|^2.$$

However, although the overall state $|\Psi'\rangle$ is normalised, the malicious agents' part of the state is not. Thus, we need to determine a bound on $\langle\psi_0|\psi_0\rangle$ and $\langle\psi_1|\psi_1\rangle$. We have:

$$F(|\Psi'\rangle, |\Phi_0^n\rangle) = |\langle\Phi_0^n|\Psi'\rangle|^2 \geq \sqrt{1-\epsilon^2}.$$

It was shown in [2] that we can write for any k, n:

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2}}\left[|\Phi_0^k\rangle|\Phi_0^{n-k}\rangle - |\Phi_1^k\rangle|\Phi_1^{n-k}\rangle\right],$$

and using this, we get:

$$\frac{1}{2}|(\langle\Phi_0^{n-k}|\psi_0\rangle)^2 + (\langle\Phi_1^{n-k}|\psi_1\rangle)^2 - 2\langle\Phi_0^{n-k}|\psi_0\rangle\langle\Phi_1^{n-k}|\psi_1\rangle| \geq \sqrt{1-\epsilon^2}.$$

Now let, $\langle\Phi_0^{n-k}|\psi_0\rangle = a$, $\langle\Phi_1^{n-k}|\psi_1\rangle = b$:

$$\begin{aligned}
&\therefore \frac{1}{2}\left|a^2 + b^2 - 2ab\right| \geq \sqrt{1-\epsilon^2}, \\
&\implies \frac{1}{2}\left\{|a|^2 + |b|^2 + 2|a||b|\right\} \geq \sqrt{1-\epsilon^2}, \\
&\implies \frac{1}{2}(|a|^2 + |b|^2)\left\{1 + \frac{2}{\left|\frac{a}{b}\right| + \frac{1}{\left|\frac{a}{b}\right|}}\right\} \geq \sqrt{1-\epsilon^2}, \\
&\implies \frac{1}{2}(|a|^2 + |b|^2)\left\{1 + \frac{2}{2}\right\} \geq \sqrt{1-\epsilon^2}, \quad \text{since } x + \frac{1}{x} \geq 2 \text{ always for real } x, \\
&\implies |a|^2 + |b|^2 \geq \sqrt{1-\epsilon^2}, \\
&\therefore |\langle\Phi_0^{n-k}|\psi_0\rangle|^2 + |\langle\Phi_1^{n-k}|\psi_1\rangle|^2 \geq \sqrt{1-\epsilon^2}.
\end{aligned}$$

Using the Cauchy-Schwarz inequality, we have:

$$\begin{aligned}\langle\psi_0|\psi_0\rangle + \langle\psi_1|\psi_1\rangle &\geq \left|\langle\Phi_0^{n-k}|\psi_0\rangle\right|^2 + \left|\langle\Phi_1^{n-k}|\psi_1\rangle\right|^2 \\ &\geq \sqrt{1-\epsilon^2}.\end{aligned}$$

Since the overall state $|\Psi'\rangle$ is normalised, we have $|\langle\chi'|\chi''\rangle| \leq 1 - \sqrt{1-\epsilon^2}$. Thus, we get our expression for fidelity as:

$$\begin{aligned}F(|\Psi_i\rangle, |\Psi_j\rangle) &= |\langle\psi_0|\psi_0\rangle + \langle\psi_1|\psi_1\rangle + \langle\chi'|\chi''\rangle|^2 \\ &\geq 1 - 2\epsilon^2,\end{aligned}$$

using,$\langle\chi'|\chi''\rangle \geq -(1 - \sqrt{1-\epsilon^2})$.

3.2 Anonymity Theorem

Theorem 4. *For shared state $|\Psi\rangle$ with $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, then the probability that the malicious agents can guess the identity of the Sender is given by::*

$$Pr[guess] \leq \frac{1}{k} + \epsilon$$

Proof:

Let there be k honest agents, each of whom could potentially be the sender. Suppose that the true sender is agent $i \in \{1, 2, \ldots, k\}$. Let $|\Psi_i\rangle$ be the global pure state (of the entire network including dishonest agents) after agent i follows the protocol (e.g., applies σ_z as required). These are the final states that the malicious agents may observe to infer who the sender is.

Let $\{\Pi_i\}_{i=1}^k$ be a POVM (positive operator-valued measure) that the adversary uses to guess the sender. Then, using theorem of total probability, the probability of correctly guessing the sender is:

$$\Pr[\text{correct guess}] = \sum_{i=1}^{k} \frac{1}{k} \mathrm{Tr}(\Pi_i |\Psi_i\rangle\langle\Psi_i|),$$

assuming that the sender is chosen uniformly at random from the k honest parties.

We now use the trace distance property to upper bound this probability.

Let $|\alpha\rangle$ be any fixed reference state (for example, any of the $\{|\Psi_i\rangle\}$). Then for each i:

$$\mathrm{Tr}(\Pi_i |\Psi_i\rangle\langle\Psi_i|) = \mathrm{Tr}(\Pi_i |\alpha\rangle\langle\alpha|) + \mathrm{Tr}(\Pi_i(|\Psi_i\rangle\langle\Psi_i| - |\alpha\rangle\langle\alpha|)).$$

We now apply the inequality:

$$|\mathrm{Tr}(A(\rho-\sigma))| \leq \|A\| \cdot D(\rho,\sigma),$$

where, $\|A\|$ denotes the trace-norm of A and $D(\rho,\sigma)$ is the distance between the states ρ,σ (fidelity between $\rho,\sigma = 1-\epsilon^2 \iff D(\rho,\sigma)=\epsilon$), and note that for a POVM element Π_i, we have $\|\Pi_i\| \leq 1$ (since $\Pi_i \leq I$). Thus:

$$\mathrm{Tr}(\Pi_i|\Psi_i\rangle\langle\Psi_i|) \leq \mathrm{Tr}(\Pi_i|\alpha\rangle\langle\alpha|) + D(|\Psi_i\rangle,|\alpha\rangle).$$

We now take the average:

$$\begin{aligned}
\Pr[\text{correct guess}] &= \sum_{i=1}^{k} \frac{1}{k}\mathrm{Tr}(\Pi_i|\Psi_i\rangle\langle\Psi_i|) \\
&\leq \sum_{i=1}^{k} \frac{1}{k}\left(\mathrm{Tr}(\Pi_i|\alpha\rangle\langle\alpha|) + D(|\Psi_i\rangle,|\alpha\rangle)\right) \\
&= \sum_{i=1}^{k} \frac{1}{k}\mathrm{Tr}(\Pi_i|\alpha\rangle\langle\alpha|) + \frac{1}{k}\sum_{i=1}^{k} D(|\Psi_i\rangle,|\alpha\rangle).
\end{aligned}$$

The first term is just :

$$\frac{1}{k}\mathrm{Tr}(\sum_{i=1}^{k}\Pi_i|\alpha\rangle\langle\alpha|) = \frac{1}{k}\mathrm{Tr}(I|\alpha\rangle\langle\alpha|) \leq \frac{1}{k}.$$

For the second term, note that by the assumption that all pairs $|\Psi_i\rangle, |\Psi_j\rangle$ satisfy $D(|\Psi_i\rangle,|\Psi_j\rangle) \leq \epsilon$, we have:

$$D(|\Psi_i\rangle,|\alpha\rangle) \leq \epsilon.$$

Therefore:

$$\frac{1}{k}\sum_{i=1}^{k} D(|\Psi_i\rangle,|\alpha\rangle) \leq \epsilon.$$

Combining both bounds, we obtain:

$$\Pr[\text{guess}] \leq \frac{1}{k} + \epsilon.$$

■

4 Device-independent GHZ Verification

First I will describe the result that leads to the new verification protocol for n-party GHZ state following [15] and then in a latter sub-section show how to make it device-independent i.e. the correctness of the verification will not depend upon the genuineness of the measurement apparatuses used in the verification protocol. Consider the following set of $n+1$ operators:

$$\hat{\mathcal{O}}_0 = \sigma_x^1 \otimes \sigma_x^2 \otimes ... \otimes \sigma_x^n$$
$$\hat{\mathcal{O}}_i = \sigma_x^1 \otimes ... \otimes \sigma_x^{i-1} \otimes \sigma_y^i \otimes \sigma_y^{i+1} \otimes \sigma_x^{i+2} \otimes ... \otimes \sigma_x^n$$

for i=1,2,...,n with the convention n+1≡1.

Now for the GHZ state $|G_0^n\rangle$ and any of the operators $\hat{\mathcal{O}}$ just defined, we have,

$$\hat{\mathcal{O}}|G_0^n\rangle = \lambda|G_0^n\rangle,$$

where, $\lambda = +1$ if $\hat{\mathcal{O}} = \hat{\mathcal{O}}_0$, otherwise $\lambda = -1$. And, each $\hat{\mathcal{O}}$ is a unitary and hermitian operator by definition, hence its eigen values are ± 1. Therefore,

$$-(n+1) \leq \left\langle \hat{\mathcal{O}}_0 - \sum_{i=1}^{n} \hat{\mathcal{O}}_i \right\rangle \leq (n+1)$$

and the upper-bound is achieved for the GHZ state $|G_0^n\rangle$ only. I will prove this result in the next subsection where I discuss the eigenvalue problem of the operator $\left(\hat{\mathcal{O}}_0 - \sum_{i=1}^{n} \hat{\mathcal{O}}_i\right)$.

Also the classical bound is given by (for odd n),

$$-(n-1) \leq \left\langle \hat{\mathcal{O}}_0 - \sum_{i=1}^{n} \hat{\mathcal{O}}_i \right\rangle_{Cl} \leq (n-1),$$

where, $\left\langle \hat{\mathcal{O}}_0 - \sum_{i=1}^{n} \hat{\mathcal{O}}_i \right\rangle_{Cl}$ is the value of the operator if we replace the Pauli matrices with local realistic value i.e. with ± 1. To prove it we note that if the $\mathcal{O}_i$-s (i=1,2,...,n) have a common sign then $\mathcal{O}_0$ will also have that common sign, analogously as was shown in the three-qubit GHZ paradox case in a previous section.

This gives a way to verify the GHZ state:

Protocol 8 (New Verification Protocol)**.** *NEW VERIFICATION*

Input: *n agents share states* $|\Psi_0\rangle, |\Psi_1\rangle, ..., |\Psi_n\rangle$

Goal: *Verify that all the states* $|\Psi_0\rangle, |\Psi_1\rangle, ..., |\Psi_n\rangle$ *are GHZ states*

---

1. *The verifier:*
   a. *selects n+1 states randomly from all of the shared states and enumerates them from 0 to n.*
   b. *broadcasts which shared state is enumerated by which number among 0 to n*

---

2. *Agent j:*
   a. *Measures* $|\psi_i\rangle$ *with his (j-th party) part of the operator* $\hat{\mathcal{O}}_i$ *and gets the outcome* $Y_{ij} \in \{+1, -1\}$

---

3. *All the Agents:*
   a. *Run parity protocol n+1 times (for each i) to calculate* $\mathcal{O}_i = \bigoplus_j Y_{ij}$
   b. *Claculate* $\mathcal{O} = \mathcal{O}_0 - \sum_{i=1}^{n} \mathcal{O}_i$

---

4. *Verification passes if:*
   $\mathcal{O} = n + 1$

Evidently GHZ state always passes the test as the POVM associated with the test is given by, $\{P_0^n, I - P_0^n\}$, where,

$$P_0^n = |G_0^n\rangle\langle G_0^n|,$$

(because the maximum value $+(n+1)$ is achievable only for a pure GHZ state) instead of $P_0^n = |G_0^n\rangle\langle G_0^n| + \frac{1}{2}I_n^0$, as was in case of the earlier verification protocol.

$$\therefore P(\rho) = Tr(P_0^n \rho) = \langle G_0^n|\rho|G_0^n\rangle = F(\rho)$$

This is the relation between probability of passing the test and fidelity of the shared state with GHZ state.

4.1 Eigenvalue problem of $\left(\hat{\mathcal{O}}_0 - \sum_{i=1}^{n} \hat{\mathcal{O}}_i\right)$

Let, $|\psi\rangle$ be an arbitrary n-party state where each party is a qubit:

$$|\psi\rangle = \sum_{b_1, b_2, ..., b_n} C_{b_1 b_2 ... b_n} |b_1 b_2 ... b_n\rangle$$

where each b_i runs from 0 to 1. Now from the properties of Pauli matrices (that σ_x only flips bit, and σ_y along with flipping bits adds a phase to the bit) and the definition of the

operators we get,

$$\hat{\mathcal{O}}_0|\psi\rangle = \sum_{b_1,b_2,...,b_n} C_{b_1b_2...b_n}|\bar{b}_1\bar{b}_2...\bar{b}_n\rangle$$
$$\hat{\mathcal{O}}_i|\psi\rangle = -\sum_{b_1,b_2,...,b_n} C_{b_1b_2...b_n}(-1)^{b_i\oplus b_{i+1}}|\bar{b}_1\bar{b}_2...\bar{b}_n\rangle$$

Hence, if we define,

$$\hat{\mathcal{O}} = \hat{\mathcal{O}}_0 - \sum_{i=1}^{n}\hat{\mathcal{O}}_i$$

we can write,

$$\hat{\mathcal{O}}|\psi\rangle = \sum_{b_1,b_2,...,b_n} C_{b_1b_2...b_n}\left(1+(-1)^{b_1\oplus b_2}+(-1)^{b_2\oplus b_3}+...+(-1)^{b_{n-1}\oplus b_n}+(-1)^{b_n\oplus b_1}\right)|\bar{b}_1\bar{b}_2...\bar{b}_n\rangle$$

Now let $C_{b_1b_2...b_n} \neq 0$ only for $b_1b_2...b_n = b'_1b'_2...b'_n$ and $b_1b_2...b_n = \bar{b}'_1\bar{b}'_2...\bar{b}'_n$; also $C_{b'_1b'_2...b'_n} = \pm C_{\bar{b}'_1\bar{b}'_2...\bar{b}'_n}$. Then,

$$\hat{\mathcal{O}}|\psi\rangle = \pm\mathcal{O}|\psi\rangle,$$

where,

$$\mathcal{O} = \left(1+(-1)^{b'_1\oplus b'_2}+(-1)^{b'_2\oplus b'_3}+...+(-1)^{b'_{n-1}\oplus b'_n}+(-1)^{b'_n\oplus b'_1}\right) \quad (4)$$
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|b'_1b'_2...b'_n\rangle \pm |\bar{b}'_1\bar{b}'_2...\bar{b}'_n\rangle),$$

i.e., $\pm\mathcal{O}$ are the eigenvalues of $\hat{\mathcal{O}}$.

Now if ($b'_1 = b'_2 = ... = b'_n = 0$ or $b'_1 = b'_2 = ... = b'_n = 1$) and $C_{b'_1b'_2...b'_n} = +C_{\bar{b}'_1\bar{b}'_2...\bar{b}'_n}$, then,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00...0\rangle + |11...1\rangle) = |G_0^n\rangle$$

and, $\mathcal{O} = n+1$, and hence,

$$\hat{\mathcal{O}}|G_0^n\rangle = +(n+1)|G_0^n\rangle.$$

For any other combination of $b'_1b'_2...b'_n$, $\mathcal{O} < (n+1)$, as is evident from the definition of $\mathcal{O}$.

Now consider the 2nd term in the definition of $\mathcal{O}$. $(-1)^{b'_1\oplus b'_2}$ is $= +1$ if $b'_1 = b'_2$ and it is $= -1$ if $b'_1 \neq b'_2$, i.e. if there is a flip while going from the bit b'_1 to bit b'_2. Now I claim that

for any combination of $b'_1 b'_2 ... b'_n$ there will always be an even number of -1-s in the RHS of $eq^n(4)$. This is because, as we traverse from the 2nd term of RHS of $eq^n(4)$ starting with b'_1 to the last term, we get an even number of flips, as we return to b'_1 itself in the last term. Therefore, $\mathcal{O}$ takes values differing by 4, because simultaneously at least two (even number) $+1$-s become -1-s.

Now if the number of parties n is odd, say $n = 5$, then the values of $\mathcal{O}$ are $n + 1$=6,2,-2, and hence the eigen values $\pm\mathcal{O}$ are 6,2,-2 (coming from the + sign) and -6,-2,2 (coming from the $-$ sign), having minimum gaping 4.

But if the number of parties n is even, say $n = 4$, then the values of $\mathcal{O}$ are $n + 1$=5,1,-3, and hence the eigen values $\pm\mathcal{O}$ are 5,1,-3 (coming from the + sign) and -5,-1,3 (coming from the $-$ sign), having minimum gaping 2.

4.2 Device Independent Verification

The measurement apparatus like $\hat{\sigma}_x$ or $\hat{\sigma}_y$ used in any quantum protocol is bought from the market. But what is the guaranty that it really is a $\hat{\sigma}_x$ or $\hat{\sigma}_y$. That means our successful verification of GHZ state hinges on the genuineness of the measurement devices used, as was in the case of our earlier verification protocol. But the new verification protocol can be made device independent, as will be shown in this sub-section following [16]. First we require a simultaneous block-diagonalization lemma that will be proved in the next sub-section.

Lemma 4. *Given two Hermitian operators A and B with eigenvalues ± 1 acting on a Hilbert space $\mathcal{H}$, there is a decomposition of $\mathcal{H}$ as a direct sum of subspaces $\mathcal{H}^i$ of dimension $d \leq 2$ each, such that both A and B act within each $\mathcal{H}^i$, that is, they can be written as $A = \oplus_i A^i$ and $B = \oplus_i B^i$, where A^i and B^i act on $\mathcal{H}^i$.*

Here A^i and B^i act on $\mathcal{H}^i$ means $\mathcal{H}^i$ is closed under the action of A^i or B^i. Now suppose $A = \hat{\sigma}_x$ (which we bought from the market, may not be a genuine one,may be of higher dimension rather than a qubit) and $B = \hat{\sigma}_y$ (which we bought from the market, may not be a genuine one) , then $A^i = \Pi^i \hat{\sigma}_x \Pi^i = \hat{\sigma}_{xi}$ and $B^i = \Pi^i \hat{\sigma}_y \Pi^i = \hat{\sigma}_{yi}$, where Π^i is the projection

operator corresponding to the subspace $\mathcal{H}^i$. Now for $\hat{\mathcal{O}} = \hat{\mathcal{O}}_0 - \sum_{i=1}^{n} \hat{\mathcal{O}}_i$ we have,

$$\begin{aligned}
\left\langle \hat{\mathcal{O}} \right\rangle &= Tr(\rho\hat{\mathcal{O}}) = Tr(\rho\hat{\mathcal{O}}.I) \\
&= Tr\left(\rho\hat{\mathcal{O}} \sum_{i_1,i_2,...,i_n} \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}\right) \\
&= Tr\left(\rho \sum_{i_1,i_2,...,i_n} \hat{\mathcal{O}}_{i_1 i_2 ... i_n} \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}\right) \\
&\quad (\because \hat{\mathcal{O}}\ \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}|\phi\rangle = \hat{\mathcal{O}}_{i_1 i_2 ... i_n} \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}|\phi\rangle\ \forall|\phi\rangle) \\
&= \sum_{i_1,i_2,...,i_n} Tr\left(\rho\hat{\mathcal{O}}_{i_1 i_2 ... i_n} \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}\ \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}\right) \\
&= \sum_{i_1,i_2,...,i_n} Tr\left(\Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n} \rho \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n} \hat{\mathcal{O}}_{i_1 i_2 ... i_n}\right) \\
&\quad (\because \hat{\mathcal{O}}_{i_1 i_2 ... i_n} \text{ is the projection of } \hat{\mathcal{O}} \text{ by the projector } \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}) \\
&= \sum_{i_1,i_2,...,i_n} q_{i_1 i_2 ... i_n} Tr\left(\rho_{i_1 i_2 ... i_n} \hat{\mathcal{O}}_{i_1 i_2 ... i_n}\right),
\end{aligned}$$

where,

$$\begin{aligned}
q_{i_1 i_2 ... i_n} &= Tr\left(\Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n} \rho \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}\right) \\
\rho_{i_1 i_2 ... i_n} &= \left(\Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n} \rho \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n}\right) / q_{i_1 i_2 ... i_n}
\end{aligned}$$

. Clearly, $q_{i_1 i_2 ... i_n} \geq 0$ and

$$\begin{aligned}
\sum_{i_1,i_2,...,i_n} q_{i_1 i_2 ... i_n} &= \sum_{i_1,i_2,...,i_n} Tr\left(\Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n} \rho\right) \\
&= Tr\left(\sum_{i_1,i_2,...,i_n} \Pi^{i_1} \otimes \Pi^{i_2} \otimes ... \otimes \Pi^{i_n} \rho\right) = Tr(I\rho) = 1.
\end{aligned}$$

$$\therefore \left\langle \hat{\mathcal{O}} \right\rangle = \sum_{i_1,i_2,...,i_n} q_{i_1 i_2 ... i_n} \left\langle \hat{\mathcal{O}} \right\rangle_{i_1 i_2 ... i_n} \qquad \left(where, \left\langle \hat{\mathcal{O}} \right\rangle_{i_1 i_2 ... i_n} = Tr\left(\rho_{i_1 i_2 ... i_n} \hat{\mathcal{O}}_{i_1 i_2 ... i_n}\right)\right)$$

Now if $\left\langle \hat{\mathcal{O}} \right\rangle$ attains the maximum value (n+1) then each $\left\langle \hat{\mathcal{O}} \right\rangle_{i_1 i_2 ... i_n} = n + 1$, as $q_{i_1 i_2 ... i_n}$-s

are probabilities that sum up to 1.

$$\therefore \rho_{i_1 i_2 ... i_n} = |\psi\rangle_{i_1 i_2 ... i_n}\langle\psi|_{i_1 i_2 ... i_n}$$
$$where,\ |\psi\rangle_{i_1 i_2 ... i_n} = \frac{1}{\sqrt{2}}(|0\rangle_{i_1}|0\rangle_{i_2}...|0\rangle_{i_n} + |1\rangle_{i_1}|1\rangle_{i_2}...|1\rangle_{i_n})$$

$$\therefore |\psi\rangle = \oplus_{i_1,i_2,...,i_n}\sqrt{q_{i_1 i_2 ... i_n}}|\psi\rangle_{i_1 i_2 ... i_n} \qquad (where, \rho = |\psi\rangle\langle\psi|)$$

Now suppose each party has a qubit ancilla state $|0\rangle'$. Now if the j-th party applies the local transformation :

$$|0\rangle_{i_j} \otimes |0\rangle'_j \rightarrow |0\rangle_{i_j} \otimes |0\rangle'_j \quad , \qquad \forall i$$
$$|1\rangle_{i_j} \otimes |0\rangle'_j \rightarrow |0\rangle_{i_j} \otimes |1\rangle'_j \quad , \qquad \forall i$$

and j runs from 1 to n, then,

$$|\psi\rangle \otimes |0\rangle'_1|0\rangle'_2...|0\rangle'_n \rightarrow |\sigma\rangle \otimes |G_0^n\rangle',$$

where, $|G_0^n\rangle'$ is the GHZ state and $|\sigma\rangle$ is some junk state. Therefore, if $\left\langle \hat{\mathcal{O}} \right\rangle$ attains the maximum value (n+1) then all the parties share a genuine GHZ state together with a junk state up to local unitary transformations. And this verification method does not require the genuineness of the $\hat{\sigma}_x$ and $\hat{\sigma}_y$-s used to build $\hat{\mathcal{O}}$ beforehand.

4.3 Proof of the simultaneous block-diagonalization lemma

The lemma stated without proof in the section "Device Independent Verification" is logically equivalent to the following lemma which I prove below following [17].

Lemma 5. *Let A_1, A_2, B_1, B_2 be orthogonal projectors on a Hilbert space $\mathcal{H}$ such that $A_1 + A_2 = \mathbb{I}$ and $B_1 + B_2 = \mathbb{I}$. Then, there exists an orthonormal basis of $\mathcal{H}$ in which all four projectors are simultaneously block-diagonal, with blocks of size 1×1 or 2×2.*

Proof. Since $A_1 + A_2 = \mathbb{I}$ and $B_1 + B_2 = \mathbb{I}$, the pairs (A_1, A_2) and (B_1, B_2) each form a binary projective measurement.

We begin by examining the operator B_1, and restrict our attention to its support, i.e., the subspace where B_1 acts as the identity. Define the positive semidefinite operators

$$X_1 := B_1 A_1 B_1, \quad X_2 := B_1 A_2 B_1.$$

Note that $X_1 + X_2 = B_1$, and both X_1 and X_2 act on the support of B_1. These operators are Hermitian and commute on this support, and hence can be simultaneously diagonalized. Let $|v\rangle$ be a simultaneous eigenvector of B_1, X_1, X_2, with $B_1|v\rangle = |v\rangle$, so $B_2|v\rangle = 0$.

We analyze three cases:

Case 1: $A_1|v\rangle = 0$. Then $A_2|v\rangle = |v\rangle$, so

$$A_1|v\rangle = 0, \quad A_2|v\rangle = |v\rangle, \quad B_1|v\rangle = |v\rangle, \quad B_2|v\rangle = 0.$$

Thus, the one-dimensional subspace $\mathrm{span}\{|v\rangle\}$ is invariant under all four projectors and corresponds to a 1×1 block.

Case 2: $A_2|v\rangle = 0$. Similarly, this yields

$$A_1|v\rangle = |v\rangle, \quad A_2|v\rangle = 0, \quad B_1|v\rangle = |v\rangle, \quad B_2|v\rangle = 0,$$

corresponding to another 1×1 block.

Case 3: $A_1|v\rangle \neq 0$ and $A_2|v\rangle \neq 0$. Define

$$|a_1\rangle := A_1|v\rangle, \quad |a_2\rangle := A_2|v\rangle.$$

Since $A_1A_2 = 0$ and $A_1 + A_2 = \mathbb{I}$, the vectors $|a_1\rangle$ and $|a_2\rangle$ are orthogonal and satisfy $|v\rangle = |a_1\rangle + |a_2\rangle$. Let

$$E_v := \mathrm{span}\{|a_1\rangle, |a_2\rangle\},$$

which is a two-dimensional subspace. Observe that

$$B_1|a_i\rangle = B_1A_i|v\rangle \propto |v\rangle \in E_v, \quad \text{for } i = 1, 2.$$

Hence B_1 maps E_v to itself, and being Hermitian, it is diagonalizable on E_v. Therefore, there exists a basis $\{|v\rangle, |w\rangle\}$ of E_v in which B_1 and hence $B_2 = \mathbb{I} - B_1$ are diagonal. Moreover, since $|a_1\rangle, |a_2\rangle \in E_v$, and A_1, A_2 act as orthogonal projectors onto these vectors, all four projectors are simultaneously block-diagonal on E_v.

Repeating this process for all simultaneous eigenvectors of $B_1, B_1A_1B_1, B_1A_2B_1$, and similarly for B_2, we obtain a decomposition of $\mathcal{H}$ into orthogonal subspaces $E_1, E_2, \ldots$, each of dimension one or two, on which all four projectors act invariantly and are diagonalizable.

Hence, in the resulting orthonormal basis formed by the union of bases of the E_i, all four projectors A_1, A_2, B_1, B_2 are simultaneously block-diagonal, with each block of size at most 2×2. □

4.4 Error Analysis of the Device-independent Scheme

Suppose the state ρ is given by :

$$\rho = \sum_k p_k |p_k\rangle\langle p_k|.$$
$$\therefore \left\langle \hat{\mathcal{O}} \right\rangle = \sum_k p_k \langle p_k|\hat{\mathcal{O}}|p_k\rangle$$

Now, suppose that $\left\langle \hat{\mathcal{O}} \right\rangle$ comes out a little less than than the maximum value (n+1):

$$\left\langle \hat{\mathcal{O}} \right\rangle = (n+1) - \epsilon$$

and let this happens because,

$$\langle p_k|\hat{\mathcal{O}}|p_k\rangle = (n+1) - \epsilon_k.$$
$$\therefore \sum_k p_k \epsilon_k = \epsilon$$

Also we can write similarly to the previous sub-section :

$$\langle p_k|\hat{\mathcal{O}}|p_k\rangle = \sum_{i_1,i_2,\ldots,i_n} q^k_{i_1 i_2 \ldots i_n} \langle \psi^k_{i_1 i_2 \ldots i_n}|\hat{\mathcal{O}}|\psi^k_{i_1 i_2 \ldots i_n}\rangle$$

where, $q^k_{i_1 i_2 \ldots i_n}$-s are probabilities that sum up to 1. Now let,

$$\langle \psi^k_{i_1 i_2 \ldots i_n}|\hat{\mathcal{O}}|\psi^k_{i_1 i_2 \ldots i_n}\rangle = (n+1) - \epsilon^k_{i_1 i_2 \ldots i_n}. \tag{5}$$
$$\therefore \sum_{i_1,i_2,\ldots,i_n} q^k_{i_1 i_2 \ldots i_n} \epsilon^k_{i_1 i_2 \ldots i_n} = \epsilon_k$$

Now let, the square root of fidelity between GHZ state and $|\psi^k_{i_1 i_2 \ldots i_n}\rangle$ be $\sqrt{1 - \delta^{k,0}_{i_1 i_2 \ldots i_n}}$. Therefore, we can expand $|\psi^k_{i_1 i_2 \ldots i_n}\rangle$ in orthonormal basis as:

$$|\psi^k_{i_1 i_2 \ldots i_n}\rangle = \sqrt{1 - \delta^{k,0}_{i_1 i_2 \ldots i_n}}|G^n_0\rangle + \sqrt{\delta^{k,1}_{i_1 i_2 \ldots i_n}}|G^n_1\rangle + \sum_{l=2}^{2^n-1} \sqrt{\delta^{k,l}_{i_1 i_2 \ldots i_n}}|G^n_l\rangle,$$

where $|G^n_1\rangle$ is the " $-$ " version of GHZ state. Due to normalization of $|\psi^k_{i_1 i_2 \ldots i_n}\rangle$ we have,

$$\delta^{k,0}_{i_1 i_2 \ldots i_n} = \sum_{l=1}^{2^n-1} \delta^{k,l}_{i_1 i_2 \ldots i_n}. \tag{6}$$

Now using this expansion of $|\psi^k_{i_1 i_2 \ldots i_n}\rangle$ into $eq^n(5)$ we get:

$$(n+1)(1-\delta^{k,0}_{i_1 i_2 \ldots i_n}) - (n+1)\delta^{k,1}_{i_1 i_2 \ldots i_n} + \langle -(n-1) \leftrightarrow (n-1)\rangle \sum_{l=2}^{2^n-1} \delta^{k,l}_{i_1 i_2 \ldots i_n} = (n+1) - \epsilon^k_{i_1 i_2 \ldots i_n}$$

where, $\langle -(n-1) \leftrightarrow (n-1)\rangle$ is some number between $-(n-1)$ and $(n-1)$, because the minimum gaping between the eigenvalues are 2 units. Simplifying we get,

$$\epsilon^k_{i_1 i_2 \ldots i_n} = (n+1)\delta^{k,0}_{i_1 i_2 \ldots i_n} + (n+1)\delta^{k,1}_{i_1 i_2 \ldots i_n} - \langle -(n-1) \leftrightarrow (n-1)\rangle \sum_{l=2}^{2^n-1} \delta^{k,l}_{i_1 i_2 \ldots i_n}$$

$$\implies (n+1)\delta^{k,0}_{i_1 i_2 \ldots i_n} - (n-1)\sum_{l=1}^{2^n-1} \delta^{k,l}_{i_1 i_2 \ldots i_n} \leq \epsilon^k_{i_1 i_2 \ldots i_n} \leq (n+1)\delta^{k,0}_{i_1 i_2 \ldots i_n} + (n+1)\sum_{l=1}^{2^n-1} \delta^{k,l}_{i_1 i_2 \ldots i_n}$$

$$\implies 2\delta^{k,0}_{i_1 i_2 \ldots i_n} \leq \epsilon^k_{i_1 i_2 \ldots i_n} \leq 2(n+1)\delta^{k,0}_{i_1 i_2 \ldots i_n} \quad (using\ eq^n(6))$$

Now as ϵ is an average of the $\epsilon^k_{i_1 i_2 \ldots i_n}$-s, so we can apply the averaging throughout to get:

$$2\delta \leq \epsilon \leq 2(n+1)\delta$$

where $(1-\delta)$ is the fidelity of the whole state ρ with the GHZ state.

$$\therefore \frac{\epsilon}{2(n+1)} \leq \delta \leq \frac{\epsilon}{2}$$

5 Quantum version of Anonymous Classical Protocols

In this section I will describe new Parity, Logical-OR (Veto) and Notification protocols that relies on the resource of shared GHZ states(that's why "Quantum" in the name of the protocols).

For parity protocol we require 1 shared GHZ state. Now to calculate parity, j-th party applies identity or $\hat{\sigma}_z$, on his part of the shared GHZ state ,accordingly if his input is 0 or 1. After this the GHZ state becomes:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00...0\rangle + e^{\left(i\pi \sum_j b_j\right)}|11...1\rangle\right) \tag{7}$$

where b_j is the input bit of j-th party. Now, $|\psi\rangle$ is GHZ state if $\sum_j b_j$ is even, i.e. even parity and $|\psi\rangle$ is the " $-$ " version of GHZ state if $\sum_j b_j$ is odd, i.e. odd parity. The agents can distinguish, whether $|\psi\rangle$ is GHZ or its " $-$ " version deterministically by the following procedure, from a single copy of $|\psi\rangle$ (which is not possible for the new verification protocol

as it requires multiple states, to be verified, as input):
Every agent measures his/her part of the shared state $|\psi\rangle$ in X-basis, and all of them simultaneously broadcast the measurement outcome ($+/-$ i.e. 0/1). Then everyone can calculate the XOR of all the simultaneously broad-casted bits and get the answer even/odd parity. The logic is same as was in the last step of the correctness proof of the section "GHZ state verification" of the old verification protocol. We can now implement Logical-OR using this quantum-parity protocol,as a subroutine, as was done in the old Logical-OR protocol.

But suppose, instead we want to calculate Logical-OR by the fully quantum method.Hence, if parity comes out t be =1 then output of Logical-OR will certainly be = 1. But if parity=0 then to distinguish between the cases :

- every one gave input =0
- even but non-zero number of parties gave input 1

we execute another run of the parity protocol but with the operator:

$$\sqrt{\hat{\sigma}_z} = \begin{pmatrix} 1 & 0 \\ 0 & exp(i\frac{\pi}{2}) \end{pmatrix} \tag{8}$$

applied in place of $\hat{\sigma}_z$. Now if the final state $|\psi\rangle$ is the "$-$" version of GHZ state then Logical-OR=1 and if it is indeed the GHZ state then another run of parity protocol is executed but now with the operator:

$$\sqrt{\sqrt{\hat{\sigma}_z}} = \begin{pmatrix} 1 & 0 \\ 0 & exp(i\frac{\pi}{2^2}) \end{pmatrix} \tag{9}$$

and so on up to maximum $\lfloor log_2 n \rfloor$ times. This process clearly reveals in some cases the partial information about the estimate of how many agents gave input 1.

To have the quantum version of Notification protocol, we can just replace its classical Parity sub-protocol with the Quantum version of parity protocol with the change that at the last step of Quantum parity protocol everyone ,except whose turn is to receive , broadcast the measurement outcome (in any order) instead of a simultaneous broadcast.

6 Conclusion and Future Work

In this report, we presented protocols for anonymous communication in quantum networks. The existing protocols use a combination of classical sub-protocols and quantum sub-protocols

for anonymous communication. We presented the existing protocols for verification or certification of GHZ state and ϵ-anonymous entanglement distribution. We created Quantum version of the Classical anonymous sub-protocols like Parity, Logical-OR, Notification. We have also provided a protocol for device-independent verification or certification of the GHZ state used in the protocols.

The ϵ-anonymity protocol ensures that the sender anonymity is preserved in a probabilistic sense; a smaller ϵ gives better anonymity. The proposed protocol is implementable in a distributed quantum network with the help of a trusted source for GHZ state. In case a trusted source is not available, our protocol for GHZ verification can be used to verify the state before using it for anonymous entanglement generation.

Future work involves detection and avoidance of collision (i.e. more than one sender or receiver) in the Quantum Notification Protocol, extending the device-independent verification of GHZ state to the case where dishonest agents are present, extending the anonymous entanglement protocol to a dynamic setting where participants may join or leave the network, and evaluating the performance of these protocols on actual or simulated quantum hardware.

References

[1] David Chaum. "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", Journal of Cryptology, vol. 1, No, 1, pp. 65-75, (1988)

[2] F. Hao, P. Zieliński, "A 2-round anonymous veto protocol", Proceedings of the 14th International Workshop on Security Protocols,pp 202–211, (2006).

[3] J. Kimble, "The quantum internet", Nature(London) 453, 1023 (2008).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev,"The security of practical quantum key distribution", Rev. Mod. Phys. 81, 1301 (2009).

[5] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan,"Practical challenges in quantum key distribution", npj Quantum Info. 2, 16025 (2016).

[6] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, "Verification of Quantum Computation: An Overview of Existing Approaches", Theory Comput. Syst. 63, 715 (2019).

[7] A. Broadbent and A. Tapp,"Information-Theoretic Security Without an Honest Majority", in Advances in Cryptology ASIACRYPT2007,edited by K. Kurosawa,Lecture Notes in Computer Science, Vol. 4833 (Springer, Berlin, Heidelberg, 2007), pp. 410–426.

[8] M. Christandl and S. Wehner, "Quantum Anonymous Transmissions",in Advances in Cryptology ASIACRYPT 2005, edited by B. Roy, Lecture Notes in Computer Science, Vol. 4833 (Springer, Berlin, Heidelberg, 2005), pp. 217–235.

[9] D. M. Greenberger, M. A. Horne, and A. Zeilinger,"Going Beyond Bell's Theorem", in Bell's Theorem, Quantum Theory, and Conceptions of the Universe, M. Kafatos (Ed.), Kluwer, Dordrecht (1989), pp. 69–72.

[10] 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. 70, 1895 (1993).

[11] V. Lipinska, G. Murta, and S. Wehner,"Anonymous transmission in a noisy quantum network using the W state", Phys. Rev. A 98, 052320 (2018).

[12] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp,"Anonymous Quantum Communication", in Advances in Cryptology– ASIACRYPT 2007, edited by K. Kurosawa, Lecture Notes in Computer Science, Vol. 4833 (Springer, Berlin, Heidelberg, 2007), pp. 460–473.

[13] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite Entanglement Verification Resistant against Dishonest Parties",Phys. Rev. Lett. 108, 260502 (2012).

[14] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, et al., "Experimental verification of multipartite entanglement in quantum networks",Nature Commun. 7, 13251 (2016).

[15] Ramij Rahaman, Guruprasad Kar, "GHZ correlation provides secure Anonymous Veto Protocol", arXiv:1507.00592

[16] Rafael Rabelo, Law Yun Zhi, Valerio Scarani, "Device-Independent Bounds for Hardy's Experiment", Phys. Rev. Lett. 109, 180401 (2012)

[17] L. Masanes, "Asymptotic Violation of Bell Inequalities and Distillability", Phys. Rev. Lett. 97, 050503 (2006).