Applications of Entanglement and Nonlocality

by

Sayan Gangopadhyay

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2021

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contribution

Sayan Gangopadhyay is the primary contributor to all aspects of this thesis. Other contributors include but are not limited to Shohini Ghose, Robert Mann, Atefeh Mashatan, Sanchit Srivastava, Amit Anand, Meenu Kumari, Tiejun Wang, Jack Davis and Hussein Abulkasim.

Abstract

Entanglement and nonlocality are two of the features demonstrated by quantum systems which give rise to new possibilities in a variety of fields such as communication technology, cryptography and the study of fundamental physics. In this thesis, we explore three such applications of entanglement and nonlocality.

In the first problem, we show that currently available noisy intermediate-scale quantum (NISQ) computers can be used for versatile quantum simulations of chaotic systems. We introduce a novel classical-quantum hybrid approach for exploring the dynamics of the chaotic quantum kicked top (QKT) on a universal quantum computer. The programmability of this approach allows us to experimentally explore the complete range of QKT chaoticity parameter regimes inaccessible to previous studies. Furthermore, the number of gates in our simulation does not increase with the number of kicks, thus making it possible to study the QKT evolution for an arbitrary number of kicks without fidelity loss. Using a publicly accessible NISQ computer (IBMQ), we observe periodicities in the evolution of the 2-qubit QKT, as well as signatures of chaos in the time-averaged 2-qubit entanglement. We also demonstrate a connection between entanglement and delocalization in the 2-qubit QKT, confirming theoretical predictions.

In the second problem, we perform a device independent study of controlled teleportation of a qubit with an untrusted receiver. We construct a device independently testable scenario in a way that allows us to certify in the context of controlled teleportation, whether quantum resources are being used by the device despite the receiver being untrusted. We find in this case that the well known Svetlichny inequality must be violated to certify quantum correlations. While a maximal violation of Mermin's inequality guarantees maximum control power in controlled teleportation with trusted parties, we find that the Svetlichny inequality must be maximally violated to guarantee maximal control power with an untrusted receiver. This indicates that a stronger form of nonlocality is required to device independently test the controlled quantum teleportation with an untrusted receiver. By taking the example of the total depolarized and the qubit depolarized GHZ states, we show that controller's authority is a monotonically increasing function of the Svetlichny inequality violation. We find a window of non-maximal Svetlichny inequality violation where the controller's authority is non-zero. This shows that the controlled teleportation scheme with an untrusted receiver is robust to depolarizing noise present in the device.

In the third problem, we study the quantum circuit implementation of a cryptographic object called quantum lightning. Quantum lightning is a strengthening of the public key quantum money scheme. We review an existing construction of quantum lightning, build

the quantum circuit implementing an important step of the scheme and identify the difficulties in realizing others.

Acknowledgements

This thesis would not have been possible without the guidance of my supervisor, Dr. Shohini Ghose. Thank you for giving me the opportunity to pursue master's studies in your research group. Your encouragement and skepticism of my research has taught me to tread steadily and carefully. I appreciate your constant support during the tough times of the past year. I would like to thank Dr. Robert Mann, my co-supervisor for supporting me in all my endeavours and letting me explore an exciting side project on relativistic quantum information. I am grateful to both my supervisors for not only being my research mentors but also for helping me grow as an individual. I would like to thank Dr. Atefeh Mashatan and Dr. Norbert Lütkenhaus for their invaluable insights and suggestions that helped me shape this thesis. This thesis was made possible by the collaboration with Cybersecurity Research Laboratory, Ryerson University (CRL) directed by Dr. Atefeh Mashatan.

I express special gratitude to Devashish Tupkary, Shlok Nahar, Dr. Tiejun Wang, Supratik Sarkar, Dr. Hussein Abulkasim, Marcus Edwards, Jack Davis and Dr. Meenu Kumari for enriching discussions. Thank you Meenu and Jack for always being available to answer my Physics questions. Thanks to the endless enthusiasm and support of Amit Anand and Sanchit Srivastava which was indispensable to this thesis.

I am grateful to my roommates for making life interesting even when the world around us looked depressed and fatigued from lockdowns. Finally, I want to thank my family for their unwavering love.

Table of Contents

List of Figures

Chapter 1

Introduction

Entanglement is a quantum phenomenon in which the description of a composite system of two or more individual systems is not the same as the sum of its constituents. Nonlocality is a more general notion according to which it is possible to observe correlations between spatially separated systems that may have interacted in the past but their past interactions do not account for the observed correlations. Though intimately related, nonlocality and entanglement are not equivalent in quantum mechanics. The relation between the two is still a topic of active research. Entanglement is widely useful in the field of quantum information science. The most popular example is perhaps the teleportation of quantum states between remote locations [9]. Quantum entanglement can in principle be used for sharing unconditionally secure keys through which secret messages can be exchanged [18]. Direct applications of nonlocality can be found in device independent quantum communication [55] and random number generation [50]. The device independent framework is a powerful application of nonlocality in which an unknown state and measurement device can be characterized [12]. In this thesis, we will explore three diverse applications of nonlocality and entanglement in the fields of chaos, communication and quantum money. First, we will review entanglement and nonlocality in some more detail.

1.1 Entanglement

Let the quantum state of a composite system of two systems A and B be ρ^{AB}. This state is said to be entangled if it cannot be expressed as the separable form:

$$\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$$

where $p_i > 0$, $\sum_i p_i = 1$, $\rho_i^A \in \mathcal{H}^A$, $\rho_i^B \in \mathcal{H}^B$, $\rho^{AB} \in \mathcal{H}^A \otimes \mathcal{H}^B$ and $\mathcal{H}^A, \mathcal{H}^B, \mathcal{H}^{AB}$ denote the Hilbert spaces of the respective systems. Now, given any quantum state, it is necessary to quantify how entangled it is for cryptographic applications and as we will see in a later chapter, to study the quantum-classical correspondence in chaotic systems. A basic measure of entanglement is the entanglement of formation. Consider all the pure state decompositions of the bipartite system comprising A and B such that $\rho^{AB} = \sum_i p_i |\psi_i\rangle \langle\psi_i|$. The measure of entanglement for a pure state $\rho = |\psi\rangle \langle\psi|$ is $E(\rho) = -\operatorname{Tr}(\rho^A \log_2 \rho^A) = -\operatorname{Tr}(\rho^B \log_2 \rho^B)$ where $\rho^{A/B} = \operatorname{Tr}^{B/A}(\rho^{AB})$. The entanglement of formation is given by $E(\rho^{AB}) = \min \sum_i p_i E(|\psi_i\rangle \langle\psi_i|)$ where the minimization is done over all pure state decompositions of ρ^{AB}. Wooters [80] showed that it is possible to derive a precise expression (without the minimization) for the entanglement of formation when ρ^{AB} is a 2-qubit state. This quantity is called concurrence and can be calculated as follows:
Define $\tilde{\rho} = \sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y$ (where σ_y is Pauli matrix and ρ^* is complex conjugate of ρ in the standard basis) is computed. Then concurrence is defined as

$$C = \max(0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}) \tag{1.1}$$

where λ_i are eigenvalues of $\rho\tilde{\rho}$ such that $\lambda_4 \leq \lambda_3 \leq \lambda_2 \leq \lambda_1$ and $0 \leq C \leq 1$. It is 0 for separable states and unity for the Bell states.

1.2 Nonlocality

Consider two systems A and B that may have interacted in the past but are now spatially separated, i.e., cannot communicate using electromagnetic signals. Alice and Bob are two distant observers who perform measurements on A and B respectively. We label Alice's measurement setting by x and Bob's measurement setting by y. We denote Alice and Bob's measurement outcome by a and b respectively. We note that for a given pair of measurement settings x and y, the outcomes a and b can be different for different rounds. By performing several rounds of measurements, the observers can estimate the probability distribution $p(ab|xy)$. Generally, the distribution cannot be factorized, i.e., $p(ab|xy) \neq p(a|x)p(b|y)$. It appears as if the outcome of each observer is not completely determined by their measurement setting and that it depends on the setting and outcome of the other observer. To explain this correlation between one observer's measurement outcome with that of the other observer's measurement setting and outcome, one may take into account the past interactions of their systems. Let us denote by λ, all factors due to past interactions that may have some causal influence on the outcomes of both

observers. Using λ, we should be able to account for the correlations, i.e., the probability distribution can be written as $p(ab|xy) = p(a|x\lambda)p(b|y\lambda)$. It is not necessary that the factor λ will be same for every run of the experiment. Therefore we must consider a distribution $p(\lambda)$ associated with the variable, λ. Now, the joint distribution of the observations can be expressed in the following factorizable form:

$$p(ab|xy) = \sum_{\lambda} p(\lambda)p(a|x\lambda)p(b|y\lambda) \tag{1.2}$$

Conditions on $p(ab|xy)$, called Bell Inequalities, are linear inequalities of $p(ab|xy)$ which must be satisfied if it admits a factorizable form as given in 1.2. In quantum mechanics there exist combinations of state, measurement settings and outcomes for which these Bell inequalities are violated. This means in some scenarios there does not exist a variable λ that explains the correlations between the observations of Alice and bob. In such a case, the joint distribution $p(ab|xy)$ characterizing their observations is called a nonlocal distribution. One example of a Bell inequality in the two-party setting described here is the famous $CHSH$ inequality. The higher the violation of this inequality the higher the nonlocality of that distribution.

It is important to note that while entanglement is a property of the quantum state, nonlocality depends on both the state and measurement operators acting on the state [12].

1.3 Overview

In Chapter 2, we study the quantum simulation of the quantum kicked top (QKT) - a periodically driven spin system that undergoes chaotic dynamics in the classical limit. We review the QKT model which can be described as the collection of a fixed number of spin-1/2 particles. We highlight the importance of entanglement in the study of quantum-classical correspondence using the QKT. After a short review of laboratory experiments implementing the QKT, we introduce a novel approach for simulating the QKT evolution on a universal quantum computer with high accuracy. We adapt our procedure to the requirements of IBM's 5-qubit quantum computer. We demonstrate that using publicly available quantum computing resources, we can simulate the evolution of QKT with higher accuracy than in experiments previously conducted in the laboratory for a large number of time periods and a wide range of its chaoticity parameter. We faithfully demonstrate previously studied periodicities in the evolution of the 2-qubit QKT. Furthermore, we report the first observation of the correspondence between average entanglement and delocalization in the 2-qubit QKT.

In Chapter 3, we study the controlled quantum teleportation of a qubit in the presence of an adversary. First we review the standard teleportation protocol and then describe the formalism of controlled teleportation protocol involving three parties. We discuss the role of nonlocality in the certification of quantum resources used for the standard teleportation protocol. Then we adapt the techniques using the notion of multipartite nonlocality to construct a device independent certification for the controlled teleportation of a qubit with an untrusted receiver. We discuss the role of Svetlichny inequality in the certification process. We numerically obtain the controller's authority for non-maximal violation of the same inequality under a specific adversarial strategy on depolarized GHZ states.

In Chapter 4, we study the quantum circuit implementation of a cryptographic object called quantum lightning. We review the concept of quantum money and discuss its strengthening, namely, quantum lightning. We describe a specific construction by Mark Zhandry, build the quantum circuit implementing an important step of the scheme involving extensive entangling operations and identify the difficulties in realizing others.

Chapter 2

Quantum Simulation of the Quantum Kicked Top

2.1 Introduction

The possibility of mapping one quantum system into another opens up new windows for efficiently exploring the properties and dynamics of general quantum systems [46, 21]. Large-scale, programmable quantum computers could offer this possibility of mapping and simulating complex quantum systems [26]. However, large-scale quantum computers have not yet been realized. Nevertheless, it is worth exploring the potential for quantum simulations using currently available noisy intermediate-scale quantum (NISQ) computers [66]. One such potential area of NISQ application is the topic of quantum chaos - the study of quantum systems that exhibit chaos in some classical limit. The question of how classical chaos emerges from quantum dynamics remains one of the open fundamental questions in quantum theory [87, 32]. On the experimental side as well, the quantum control and precision needed to explore quantum chaotic dynamics over a wide range of parameters and long time scales remains quite challenging. So far, relatively few experiments in limited parameter regimes and for short times have been performed [48, 73, 15, 42, 59]. In this chapter, we demonstrate the use of NISQ computers for flexible simulations of quantum chaos.

In classical mechanics, the chaotic behaviour of a system is characterized by unpredictability in evolution due to exponential sensitivity to initial conditions. Classical chaos is quantified by the Lyapunov exponent that is a measure of the rate of divergence of neighbouring trajectories [20, 62]. A corresponding quantum measure of chaos is challenging to

define due to the uncertainty principle and the linearity of quantum evolution. Entanglement, on the other hand, is an entirely quantum phenomenon by which physical systems are correlated in a 'spooky' way. The connection between the seemingly different notions of chaos and entanglement has eluded physicists for decades. One way to relate classical mechanical concepts to quantum mechanics is by invoking Bohr's quantum-classical correspondence principle which states that quantum mechanics reproduces classical mechanics (*including chaos*) in the limit of large quantum numbers. However, the correspondence principle breaks down for chaotic systems. The question of quantum-classical correspondence in classically chaotic systems has been explored in the context of quantum information processing and has gained relevance for quantum computing applications. It has been shown that classical chaos can affect the implementation of quantum computing algorithms [25, 24]. Chaos can also affect the generation of dynamical entanglement, an important resource for quantum computing.

To understand chaos in the quantum context, it is important to explore signatures of classical chaos in the deep quantum regime, where the standard Bohr correspondence principle cannot be invoked. A frequently used model for studying quantum chaos is the quantum kicked top [34], which is a finite-dimensional spin system that displays chaotic dynamics in the classical limit. The quantum kicked top (QKT) has been extensively studied theoretically [54, 29, 77, 11, 27, 70]. The system can be described as a collection of indistinguishable qubits, which makes it attractive to explore in the framework of quantum information processing and NISQ devices.

In the deep quantum regime, periodicities and symmetries in the two- and three-qubit QKT model were studied theoretically [11, 70]. A few experimental studies of the QKT have also been performed [42, 15, 59]. In [59], a 3-qubit model of the QKT was shown to exhibit ergodic dynamics and a resemblance between entanglement entropy and classical phase space dynamics was noted. Temporal periodicity and symmetries of the 2-qubit QKT were explored using NMR techniques in [42]. These experiments are limited to a small number of kicks and a small range of chaoticity parameter (κ), due to decoherence in the physical qubits. To experimentally study the long term dynamics and dependence on κ rigorously, one needs to explore longer time scales and a wider range of κ. In this work, we show that mapping the QKT onto a programmable quantum circuit in a quantum computer allows simulations of the QKT that overcome previous experimental limitations. This opens new regimes of experimental exploration in both time and parameter space.

We construct and demonstrate for the first time, an exact simulation of the 2-qubit quantum kicked top using a universal set of quantum logic gates. Our quantum circuit-based simulation is programmable and enables flexible initial state preparation and evolution. Using IBM's 5-qubit chip Vigo, we can prepare initial states and implement the

dynamics of the QKT for an arbitrary number of kicks and a wide range of κ. The number of gates required for this simulation is independent of the number of kicks and value of κ. Therefore, our model does not suffer any systematic loss of fidelity with an increasing number of kicks or κ values. Finally, full quantum state tomography enables us to explore signatures of chaos in 2-qubit entanglement.

The ability to vary κ and the number of kicks allows us to experimentally observe the periodic nature of the dynamics with respect to κ as well as kick number. Additionally, the temporal periodicity of the QKT can be used to obtain highly accurate time averages of relevant physical quantities. In particular, we explore the time-averaged entanglement for different initial spin coherent states (SCS). We find that a contour plot of the time average entanglement shows clear signatures of the classical phase space structures of regular islands in a chaotic sea, even in a deep quantum regime. We also show that the states initialized in chaotic regions of the phase space show intermediate values of average concurrence, whereas, the fixed points and the period-4 orbit correspond to the minimum and maximum values respectively. This behaviour is related to the degree of delocalization of the state and thus demonstrates a connection between delocalization and entanglement [43].

Our work shows that current quantum computers are useful for flexibly exploring new experimental regimes in quantum chaotic systems. Mapping the system onto a tunable quantum circuit lets us probe different aspects of the QKT dynamics without the need for building sophisticated customized hardware or being constrained by fixed system parameters. This method combines the ease of numerical simulation with the built-in quantum evolution of a physical system.

2.2 Background

2.2.1 The Quantum Kicked Top Model

The Quantum kicked Top (QKT) model was first introduced by Haake, Kus and, Scharf in 1987 [34]. The quantum kicked top is a time-dependent periodic system governed by the Hamiltonian.

$$H = \hbar\frac{pJ_y}{\tau} + \hbar\frac{\kappa J_z^2}{2j}\left(\sum_{n=-\infty}^{n=\infty}\delta(t-n\tau)\right) \tag{2.1}$$

where J_x, J_y and J_z are angular momentum operators satisfying $[J_i, J_j] = \mathrm{i}\epsilon_{ijk}J_k$. The Hamiltonian commutes with J^2 , i.e., $[H, J^2] = 0$. Thus the eigenvalue of J^2, $j(j+1)\hbar^2$ is a constant of motion. The sum over delta functions means application of J_z^2 at intervals of τ, which will be referred to as kicks. The J_y term can be interpreted as a rotation around the y-axis.

The classical map for the kicked top can be obtained by writing the Heisenberg equations of motion for the angular momentum operators and then taking the limit $j \to \infty$. By defining the normalized variables $X = J_x/j$, $Y = J_y/j$ and $Z = J_z/j$, the classical equations of motions for $p{=}\pi/2$ are

$$\begin{aligned} X_{n+1}(\tau) &= Z_n(\tau)\cos(\kappa X_n(\tau)) + Y_n(\tau)\sin(\kappa X_n(\tau)), \\ Y_{n+1}(\tau) &= Y_n(\tau)\cos(\kappa X_n(\tau)) - Z_n(\tau)\sin(\kappa X_n(\tau)), \\ Z_{n+1}(\tau) &= -X_n(\tau) \end{aligned} \tag{2.2}$$

Here the dynamical variables (X,Y,Z) satisfy the constraint $X^2 + Y^2 + Z^2 = 1$, i.e., they are restricted to be on the unit sphere S^2. Thus, the variables can be parameterized into spherical polar coordinates as $(X, Y, Z) = (\sin(\theta)\cos(\phi), \sin(\theta)\sin(\phi), \cos(\theta))$.

As the chaoticity parameter κ is varied , the classical dynamics ranges from fully regular motion (for $\kappa \leq 2.1$) to a mixture of regular and chaotic behaviour for different initial conditions (for $2.1 \leq \kappa \leq 4.4$) to fully chaotic motion (for $\kappa > 4.4$). The classical stroboscopic map (in polar co-ordinates) for a range of initial conditions with κ =2.5 is given in Fig. 2.1. The regular regions of the phase space are composed of periodic orbits. Period-N orbits and fixed points are obtained from solutions to the equation $F^N(X, Y, Z) = (X, Y, Z)$ where F is the classical map for one period. the fixed points $FP1 = (0, -1, 0)$, $FP2 = (0, 1, 0)$ and the period-4 orbit $P4 = (1, 0, 0) \to (0, 0, -1) \to (-1, 0, 0) \to (0, 0, 1) \to (1, 0, 0)$ exist for all values of κ.

The QKT model with total angular momentum j can be thought of as a collection of $2j$ qubits.

$$J_\alpha = \frac{1}{2}\sum_{i=1}^{2j}\sigma_{i\alpha}, \quad \alpha \in \{x, y, z\}, \tag{2.3}$$

where $\sigma_{i\alpha}$ means σ_α operation on i^{th} qubit and $\mathbb{I}_2$ on the rest of the qubits. Substituting J_α in equation 2.1, we get

$$H = \hbar\frac{\kappa}{8j}\left(2j + \sum_{\substack{i,k=1 \\ i\neq k}}^{2j}\sigma_{iz}\otimes\sigma_{kz}\right)\sum_{n=-\infty}^{\infty}\delta(t - n\tau) + \hbar\frac{p}{2\tau}\sum_{i=1}^{2j}\sigma_{iy} \tag{2.4}$$

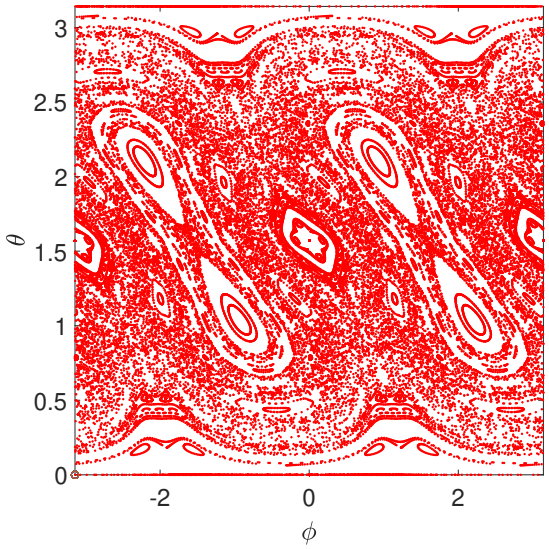


Figure 2.1: Stroboscopic phase space after 150 kicks for k=2.5 and 289 initial points in phase space.

The periodic evolution of the QKT can be described by the evolution operator from kick to kick, also called the Floquet operator U. It can be derived from the Hamiltonian H by separating H into two distinct time segments. During the first time segment $n\tau < t < (n+1)\tau - \Delta\tau$ only the rotation part $\hbar\frac{p}{\tau}J_y$ acts. During the second short time interval of $\Delta\tau$, both the rotation part ($\hbar\frac{p}{\tau}J_y$) and the kick part ($\hbar\frac{\kappa}{2j\Delta\tau}J_z^2$) act.

$$H = \begin{cases} \hbar\frac{p}{\tau}J_y, & n\tau < t < (n+1)\tau - \Delta\tau \\ \hbar\frac{p}{\tau}J_y + \hbar\frac{\kappa}{2j\Delta\tau}J_z^2, & (n+1)\tau - \Delta\tau < t < (n+1)\tau \end{cases}$$

in the limit $\Delta\tau \to 0$. The Floquet time evolution operator for one time period, τ, can be calculated as follows [43]:

$$
\begin{aligned}
U &= \lim_{\Delta\tau\to 0} U(\tau, \tau-\Delta\tau)U(\tau-\Delta\tau, 0) \\
&= \lim_{\Delta\tau\to 0} \exp\left(-\frac{\mathrm{i}}{\hbar}\int_{\tau-\Delta\tau}^{\tau}\left(\hbar\frac{p}{\tau}J_y + \hbar\frac{\kappa}{2j\Delta\tau}J_z^2\right)dt\right)\exp\left(-\frac{\mathrm{i}}{\hbar}\int_0^{\tau-\Delta\tau}\left(\hbar\frac{p}{\tau}J_y\right)dt\right) \\
&= \lim_{\Delta\tau\to 0} \exp\left(-\mathrm{i}\left(\frac{p}{\tau}J_y\Delta\tau + \frac{\kappa}{2j}J_z^2\right)\right)\exp\left(-\mathrm{i}\frac{p}{\tau}J_y(\tau-\Delta\tau)\right) \\
&= \exp\left(-\mathrm{i}\frac{\kappa}{2j}J_z^2\right)\exp\left(-\mathrm{i}pJ_y\right) \qquad (2.5)
\end{aligned}
$$

The final state $|\psi(N)\rangle$ after N kicks is obtained by applying the Floquet operator N times on the initial state $|\psi(0)\rangle$, i.e., $|\psi(N)\rangle = U^N|\psi(0)\rangle$.

For the 2-qubit QKT ($j = 1$), substituting J_α from Eq. 2.3 in Eq. 2.5 we obtain

$$
U(j=1) = \exp\left(-i\frac{\kappa}{4}(\mathbb{I}+\sigma_z\otimes\sigma_z)\right)\exp\left(-i\frac{p}{2}(\sigma_y\otimes\mathbb{I}+\mathbb{I}\otimes\sigma_y)\right). \qquad (2.6)
$$

2.2.2 Initial States

Minimum uncertainty states in spin systems are called spin coherent states (SCS) [67]. They satisfy the uncertainty relation

$$
\Delta J_i \Delta J_k = \frac{\hbar}{2}|\Delta J_l| \qquad (2.7)
$$

where i, k and l are permutations of x, y and z. The uncertainty for these states is distributed symmetrically over the two operators. For larger j values the SCS becomes highly localized around the point (θ, ϕ) in the phase space and hence in the classical limit of $j \to \infty$ approximates the classical angular momentum state (θ, ϕ) [32].

Spin squeezed states, which have asymmetric distribution of uncertainty, can display entanglement in the corresponding multi-qubit representation [52]. Since we are interested in studying entanglement which arises from the dynamics of the system, we choose SCSs as our initial states. Given any point (θ, ϕ) in the classical phase space, we construct the corresponding SCS $|j;\theta,\phi\rangle$ as

$$
|j;\theta,\phi\rangle = \exp[i\theta(J_x\sin\phi - J_y\cos\phi)]\,|j,j\rangle\,. \qquad (2.8)
$$

In the 2j-qubit space, we define our initial states as the SCSs

$$|j;\theta,\phi\rangle = |\theta,\phi\rangle^{\otimes 2j} \tag{2.9}$$

where $|\theta,\phi\rangle$ are points on the Bloch sphere.

2.2.3 Husimi Distribution

To study quantum-classical correspondence in the quantum kicked top, its Husimi distribution is often compared with the classical phase space distribution [44]. The Husimi distribution has also been used as a visual aid to study dynamical tunneling in the same model [17]. The Husimi distribution $Q(\theta,\phi)$ is given by the following equation.

$$Q(\theta,\phi) = \frac{2j+1}{4\pi} \langle\theta,\phi|\,\rho\,|\theta,\phi\rangle \tag{2.10}$$

which is equal to $\frac{2j+1}{4\pi}|\langle\theta,\phi|\psi\rangle|^2$ for pure states; the overlap of a pure angular momentum state $|\psi\rangle$ and spin coherent state $|\theta,\phi\rangle$.

2.2.4 Concurrence as a Measure of Entanglement

Entanglement of formation is the most widely accepted measure of entanglement [19]. For a mixed state ρ, it is the minimum average von Neumann entropy over all pure-state decompositions of ρ. Due to the practical difficulty of computing such an infimum, another measure of entanglement - concurrence- is more popular for quantifying entanglement in bipartite qubit systems. Concurrence is both easier to compute and is a monotonically increasing function of entanglement of formation. Concurrence is computed as follows [81]:

For a two-qubit density matrix ρ, first the spin flipped state $\tilde{\rho} = \sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y$ (where σ_y is Pauli matrix and ρ^* is complex conjugate of ρ in the standard basis) is computed. Then concurrence is defined as

$$C = \max(0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}) \tag{2.11}$$

where λ_i are eigenvalues of $\rho\tilde{\rho}$ such that $\lambda_4 \leq \lambda_3 \leq \lambda_2 \leq \lambda_1$ and $0 \leq C \leq 1$. It is 0 for separable states and unity for the Bell states.

The connection between entanglement and chaos has been long debated in the literature. Several studies [51, 29, 15, 59] showed higher time-averaged entanglement in chaotic

regions compared to regular regions in the deep quantum regime of the QKT ($j = 3/2, 3, 4$). However, some studies provided instances where even regular regions led to high entanglement in the deep quantum regime. It remained unclear how entanglement and chaos are related in the regular regions of the QKT evolution until Kumari and Ghose [45] resolved the seemingly conflicting studies. They presented the trace distance of the evolved state from SCSs as an upper bound to the bipartite entanglement of the QKT with total angular momentum j. The trace distance can be inferred from localized vs. delocalized evolution in the Husimi distribution. Thus, the entanglement degeneration in the QKT can be explained by considering whether it evolves in a localized or delocalized manner in the Husimi phase space.

2.3 Experimental Implementations in Literature

The first experimental implementation of the QKT was reported in 2009 [15]. The $j = 3$ hyperfine ground state of the ^{133}Cs atom was used to study quantum-classical correspondence in the QKT. The nonlinear rotation was performed by interacting the atom with monochromatic laser field. The kicks were realized by sequential short magnetic pulses. The value of κ in the non-linear part depends on the atomic structure, the frequency of laser field and the rate of photon scattering events. It is necessary to keep the photon scattering events low enough to minimize decoherence. This required κ to be as small as possible in the experiment.

The QKT as a collection of qubits was implemented in [15], [42]. In [59], a three-qubit ring of planar transmons with tunable inter-qubit coupling was used as the physical platform to study ergodic dynamics in the QKT. The linear rotation of each qubit was performed using a resonant microwave pulse. The nonlinear rotation was performed by turning the inter-qubit coupling circuit on/off using three square- shaped pulses. Thus, a particular pulse sequence was repeated N times to obtain the N-kick evolution. The value of κ is proportional to the interaction time of the three qubits. Higher interaction time leads to faster decoherence, as demonstrated in figure S10 of the supplementary of [59]. Thus, even this experiment is limited to low values of κ. In [42], a two-qubit implementation of the QKT on NMR qubits was achieved. Quantum-classical correspondence, symmetries and temporal periodicities of the 2-qubit kicked top were studied experimentally on the NMR qubits. The nonlinear part of the QKT hamiltonian naturally occurs in a pair of weakly coupled heteronuclear NMR qubits. The linear part is applied using short radio-frequency pulses. κ is determined by the interval between successive radio pulses. Longer time intervals correspond to larger κ and higher experimental errors.

All the experiments described have two drawbacks in common. They are limited to lower values of κ and a low number of kicks. The plots of fidelity between the experimentally reconstructed state and the classically simulated state after the N^{th} kick in [59], [42] explicitly show a steady decline. The common approach of realizing the final state after the N^{th} kick has been to repeatedly apply a set of operations such as a pulse sequence N times. This approach leads to the accumulation of experimental errors and subsequently low fidelities. If one wishes to physically prepare the evolved QKT state after arbirtarily many kicks and for an arbitrary value of κ, this approach is not suitable.

2.4 Implementation of Unitary as Quantum Gates

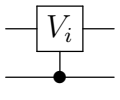
Any n-qubit unitary can be decomposed into at most $2^n(2^n-1)/2$ fully controlled single-qubit gates [76]. An alternate decomposition scheme that uses fewer controls compared to that in [76], was presented in [47]. Quantum gates with fewer controls are easier to implement. Fully controlled quantum gates involve the highest number of inter-qubit interactions which introduce errors. We choose the decomposition scheme given in [47] with a reduced number of controlled gates to ensure high accuracy of the quantum circuit implementation of the 2-qubit unitary, $U^N(j=1)$.

Under this scheme, any 4 by 4 unitary matrix U can be expressed as

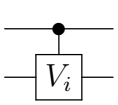
$$U = U_1 \times U_2 \times U_3 \times U_4 \times U_5 \times U_6 \tag{2.12}$$

where '$\times$' denotes matrix multiplication and U_i are two-level unitaries of the following forms

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & v_{11} & v_{12} \\ 0 & 0 & v_{21} & v_{22} \end{pmatrix} \equiv$$

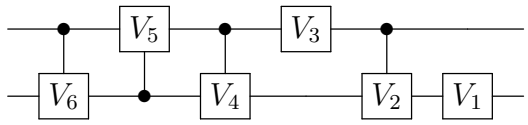


$$; \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & v_{11} & 0 & v_{12} \\ 0 & 0 & 1 & 0 \\ 0 & v_{21} & 0 & v_{22} \end{pmatrix} \equiv$$



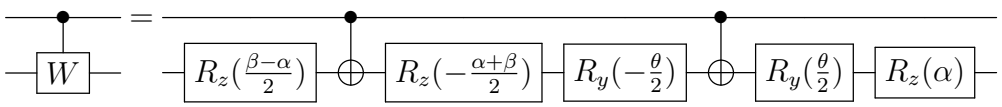
$$\begin{pmatrix} v_{11} & v_{12} & 0 & 0 \\ v_{21} & v_{22} & 0 & 0 \\ 0 & 0 & v_{11} & v_{12} \\ 0 & 0 & v_{21} & v_{22} \end{pmatrix} \equiv \mathbb{I} \otimes V_i; \quad \begin{pmatrix} v_{11} & 0 & v_{12} & 0 \\ 0 & v_{11} & 0 & v_{12} \\ v_{21} & 0 & v_{22} & 0 \\ 0 & v_{21} & 0 & v_{22} \end{pmatrix} \equiv V_i \otimes \mathbb{I}.$$

A general 1-qubit unitary can be expressed as $V_i = e^{i\delta}W$, where W$\in$ SU(2) is of the form $\begin{pmatrix} z & -w^* \\ w & z^* \end{pmatrix}$ for $w, z \in \mathbb{C}$ and $|w|^2 + |z|^2 = 1$. The exact decomposition for a 2-qubit gate in this scheme is given by the following circuit:

$U =$ 

(2.13)

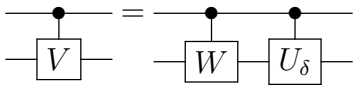
Implementation of these gates on a quantum computer requires further decomposition into rotations and CNOT gates. Given a 1-qubit unitary W$\in$ SU(2), a controlled gate of the form $(|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes W)$ can be decomposed as



(2.14)

where R_x, R_y and R_z describe rotations on the Bloch sphere and α, β and θ are such that $R_z(\alpha)R_y(\theta)R_z(\beta) = W$.

A 2-qubit gate of the form $(|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes V)$ can be written as

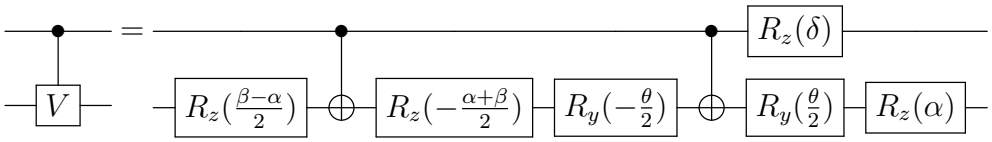


(2.15)

where $U_\delta = \exp(-i\delta) \times \mathbb{I}$. This controlled phase gate can be further simplified by moving the phase to the other qubit:

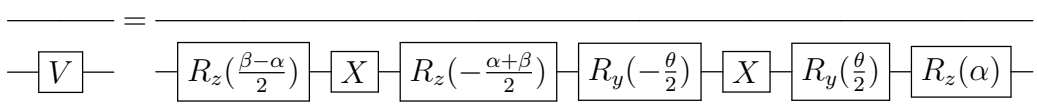
$$\begin{aligned} (|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_\delta) &= (|0\rangle\langle 0| \otimes \mathbb{I} + \exp(i\delta)\,|1\rangle\langle 1| \otimes \mathbb{I}) \\ &= (|0\rangle\langle 0| + \exp(i\delta)\,|1\rangle\langle 1|) \otimes \mathbb{I} \\ &= R_z(\delta) \otimes \mathbb{I}. \end{aligned} \tag{2.16}$$

Here, we have dropped a global phase factor of $\exp(i\delta/2)$ in the final step. Hence, we get:



(2.17)

A similar analysis follows when the control and target qubits are exchanged. For two-level unitaries of the type $\mathbb{I} \otimes V$ and $V \otimes \mathbb{I}$, the phase factors appearing on V are global and can be ignored. These gates have a similar decomposition as the one shown in Eq. (2.17) with the CNOT gates replaced by X gates. For example, a two-level unitary of the form $\mathbb{I} \otimes V$ will be decomposed as:



(2.18)

At most 46 gates, with 8 2-qubit CNOT gates and 38 single qubit rotations are required to implement a general 4 by 4 unitary under this scheme. Consecutive rotations have been counted as separate single qubit gates. Depending on the universal gate set for the particular quantum computer, the actual number of gates required may be fewer.

2.5 Implementation of Unitary on IBMQ

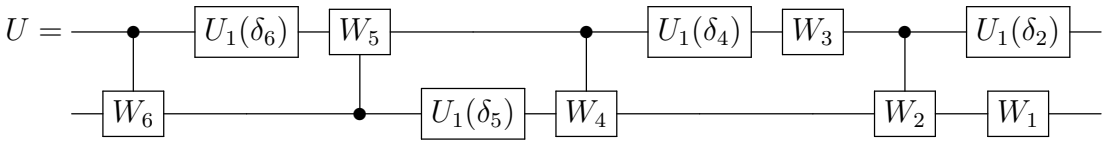
We implemented our quantum circuits on the quantum hardware and simulator backend of the IBM Quantum Experience [74]. The interfacing with the quantum hardware was done using Qiskit [1].

Qiskit allows us to implement 1-parameter and 3-parameter single-qubit unitary operators of the form

$$U_3(\theta, \phi, \lambda) = \begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i\lambda+i\phi}\cos(\theta/2) \end{pmatrix}$$

$$U_1(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix}.$$

We decomposed the gates in Eq. (2.13) into a combination of U_1 and U_3 gates. Gates of the form $V \otimes \mathbb{I}$ and $\mathbb{I} \otimes V$ were implemented directly as U_3 gates. For controlled gates, the decomposition given in Eq. (2.15) was implemented, where W$\in$ SU(2) is a U_3 gate and U_δ is a $U_1(\delta)$. Hence, we obtained the final circuit decomposition for our 2-qubit Floquet operator on IBMQ as:



(2.19)

with $W_i = U_3(\theta_i, \phi_i, \lambda_i)$.

Time evolution after multiple kicks was calculated by applying the Floquet unitary on the initial state repeatedly. This could be achieved by appending the set of gates given in Eq. (2.19) consecutively N times to simulate evolution by N steps. However, to mitigate the errors that may arise from the increasing number of gates, in our approach, we decomposed the effective N-kick unitary U^N using the same procedure as mentioned above. This means that the state after any arbitrary number of steps can be obtained by applying the same set of gates given in Eq. (2.19) with appropriate parameters. Similarly, different values of κ were simulated by computing the relevant parameters for the set of gates corresponding to the unitary $U^N(\kappa)$. This allows easier and precise control over this parameter than other qubit-based realizations of this model, where the value of κ is set by tuning the time duration of interactions between the physical qubits.

After applying the appropriate set of gates to the initial states, the final state's density matrix was constructed using state-tomography circuits built into Qiskit. Physical quantities of interest can be calculated from this density matrix. There will be discrepancies in these physical quantities between theoretical values and the experimentally obtained values from the quantum computer. Higher the depth of the quantum circuit, higher the experimental error. These errors can be due to both statistical fluctuations and systematic errors in the hardware implementation [22]. Relaxation and decoherence of the qubits in a noisy environment is a major source of systematic errors. The CNOT gate, which involves two-qubit operations is ten times as noisy as the single qubit rotations. This is because of higher errors introduced by unwanted qubit interactions during the implementation of multiqubit operations. There are also read-out errors introduced by the final quantum measurement process. These errors could be theoretically modeled and the experimental data could be filtered to account for those errors. Quantum error correcting circuits could also be used to mitigate the systematic errors. This could lead to better agreement between theoretical and experimental values of the physical quantities like concurrence. However, we do not investigate error mitigation in this thesis.

The error calibration of various gates that can be implemented on IBMQ devices is done daily and is available on their website. Using thoretical error models and these gate-error values, one could compare the suitability of different quantum computers around the

world for implementing the evolution of the 2-qubit QKT. We have not undertaken such an endeavour in this thesis.

2.6 Comparison with Previous Experiments

Starting with various initial points for two different values of κ, we have applied the quantum circuit for implementing N-kicks. We reconstructed the experimental final state by performing quantum state tomography. We use the fidelity of the reconstructed state as a measure of experimental accuracy. For the theoretical density matrix ρ_{th} and the reconstructed matrix ρ_{exp}, fidelity is given by $F(\rho_{\text{exp}}, \rho_{\text{th}}) = (\text{tr}\big(\sqrt{\sqrt{\rho_{\text{th}}}\rho_{\text{exp}}\sqrt{\rho_{\text{th}}}}\big))^2$. We observed that there is no systematic loss in fidelity with the number of kicks for different initial states and values of κ [Fig. 2.3]. Starting with initial SCS states centred at fixed points, periodic orbits and the chaotic sea of the phase space generated for κ in the range [0.5, 6.5], we averaged the $F(\rho_{\text{exp}}, \rho_{\text{th}})$ corresponding to each kick. As seen in Fig. 2.2, the average fidelities remain around 0.87.

To obtain a benchmark of how well our proposed circuit method can be implemented by a publicly accessible quantum computer (IBM Vigo), we have compared the experimental fidelities with that of [59], [42]. In [59], a monotonically decreasing fidelity with the lowest of 0.6 for 10 kicks. In [42], a significant drop in fidelity from 6^{th} to 8^{th} kick with the lowest of 0.8 was reported. In our study, the non-decreasing trend in fidelity can be attributed to the fixed number of gates for an arbitrary number of kicks. By decomposing the unitary into elementary quantum gates, we effectively remove any constraints on the parameters of the physical system (QKT) that we can implement. In the IBM-Q systems, the error varies only with the number of single-qubit physical rotations and CNOT gates acting on each qubit. Since the number of gates in the circuit remains constant irrespective of the value of κ, we see that the fidelity values do not depend on κ.

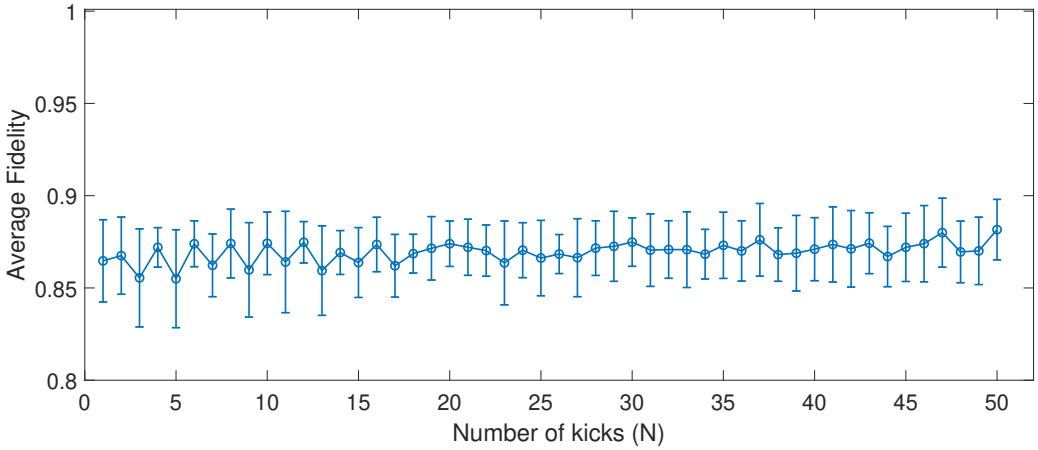


Figure 2.2: Experimental Fidelity of $U^N(\kappa)\left|\psi_{(\theta,\phi)}\right\rangle$ averaged over $(\theta,\phi) \in \{(2.25,0),(\pi/2,\pi/2),(\pi/2,0)\}$ and $\kappa \in \{0.5,2.5,4.5,6.5\}$ for the 2-qubit quantum kicked top implementation using the proposed circuit method on IBM Vigo. The error bars indicate standard deviation.

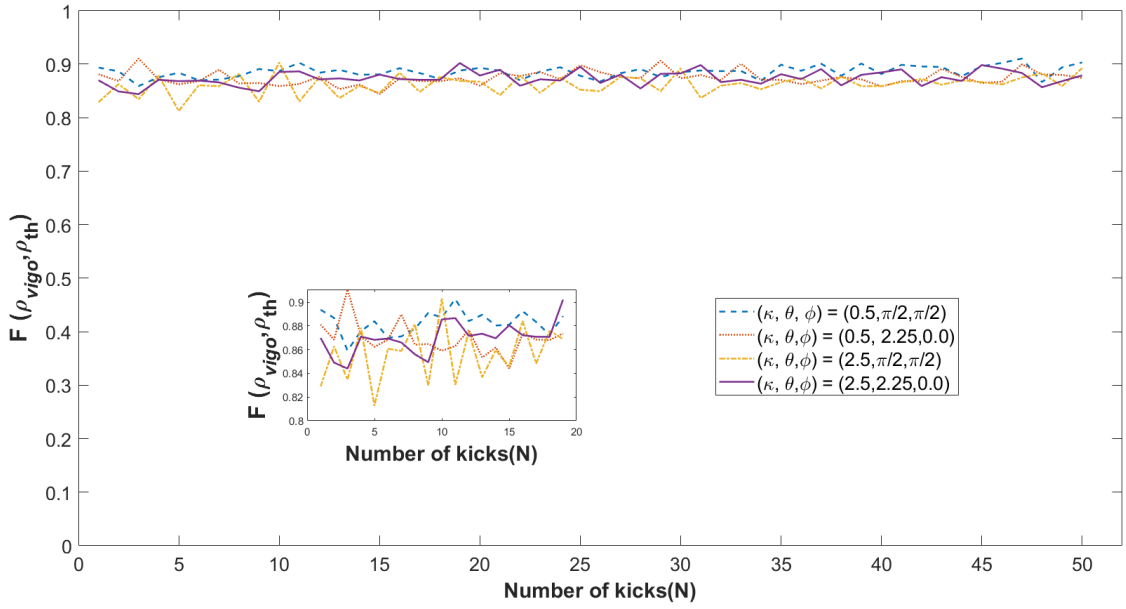


Figure 2.3: Fidelity of the tomographically reconstructed 2-qubit state for different initial states and different κ values on IBM Vigo

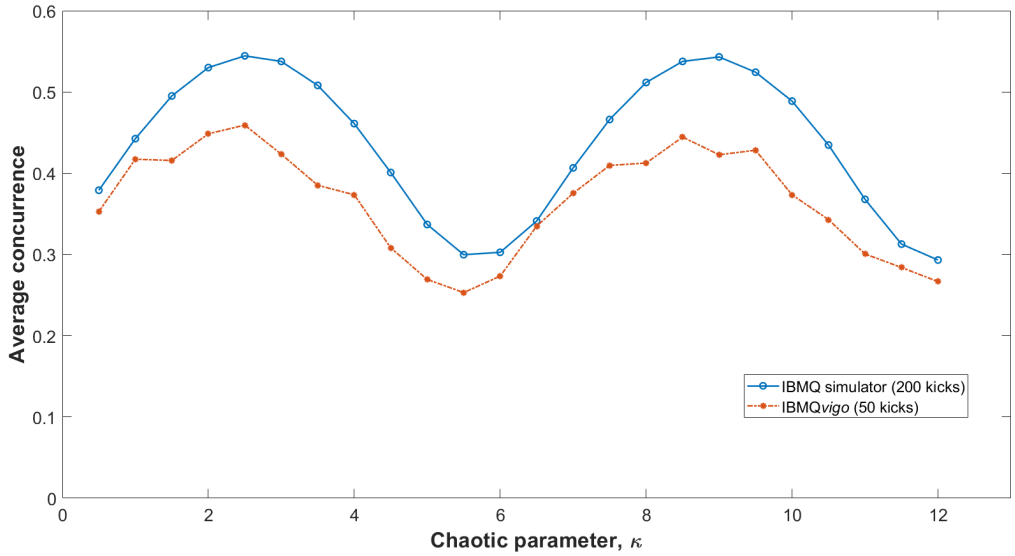
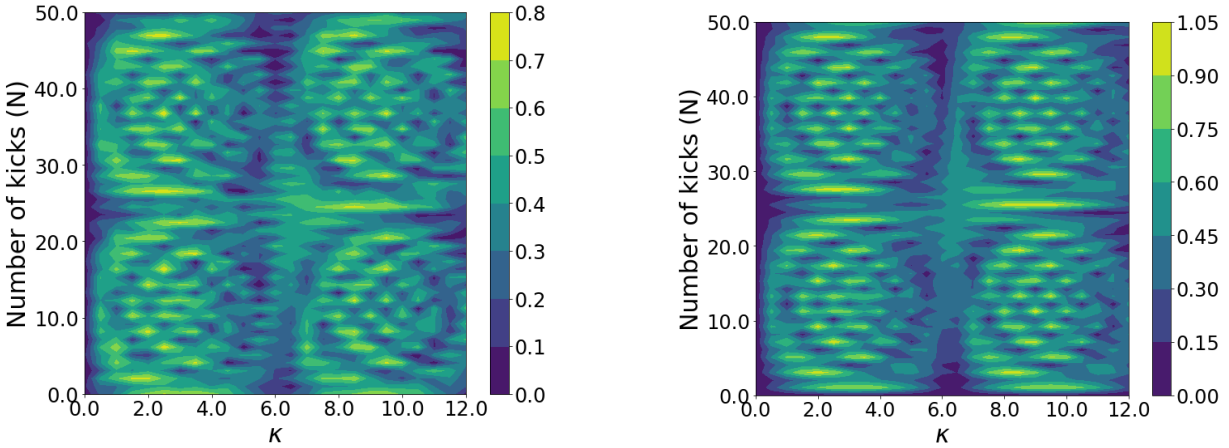


Figure 2.4: Average concurrence plotted against κ show a periodicity of 2π. The initial state was an SCS with $\theta = 2.25$ and $\phi = 2.0$.The average was taken over 200 steps for the simulated plot and over 50 steps on IBM Vigo.



(a) (b)

Figure 2.5: **a**.A contour plot of concurrence for 50 kicks over different values of κ on IBMQ-Vigo. **b**. A contour plot for concurrence over 50 kicks for different values of κ on IBMQ simulator

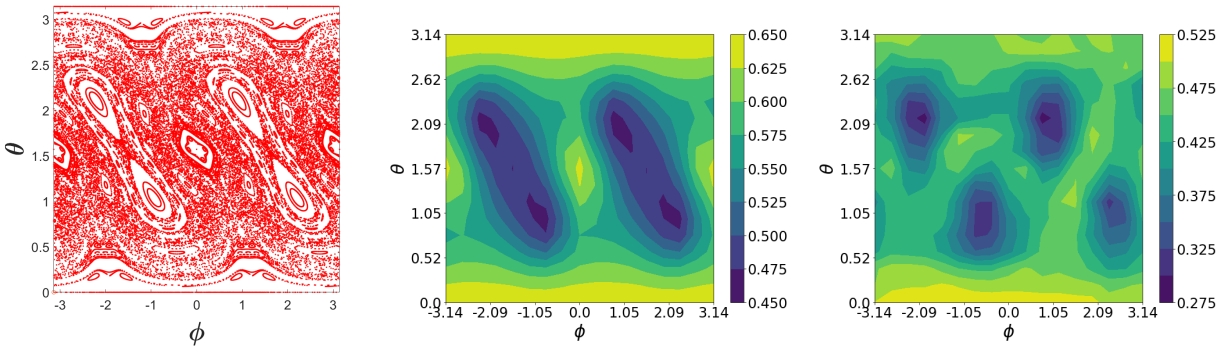
In 2018, Bhosale and Santhanam [11] had shown that for a fixed value of j and a given initial state, quantum correlations quantified by concurrence are periodic in κ, with a period of $2j\pi$. This implies that in the classical limit ($j \to \infty$), the time period of quantum correlations becomes infinite. Therefore, these correlations are no longer periodic in the classical limit. The periodic nature of concurrence is an indicator that the kicked top is either in the semi-classical or the quantum regime. In the same paper [11], it was shown that the 2-qubit kicked top shows periodicity of concurrence not only in the parameter κ but also in the number of kicks. The two-way periodic nature of the $j = 1$ QKT makes it an interesting special case of the deep quantum regime.

To our knowledge, the periodicity of quantum correlations in the 2-qubit QKT model was explored experimentally in only one previous study by Krithika et al. In [42], they had considered four different values of κ and 8 kicks for each value of κ to argue that the Husimi distribution resembles its counterpart after the expected period in κ corresponding to every kick. In this chapter, we have taken 25 different values of κ ranging from 0 to 12, and for each value of κ, we averaged the concurrence of the QKT state for 50 kicks on the quantum hardware. As shown in Fig. 2.4, the simulated and experimental results show close agreement and the periodicity of average concurrence in κ is conspicuous in the experimentally obtained plot. Thus, we have obtained a more accurate experimental realization of quantum correlations' periodicity with the chaoticity parameter, κ, in the 2-qubit kicked top. The value of concurrence has been plotted against the number of kicks and κ in the form of contour plots in Fig. 2.5a, 2.5b. Periodic nature can be observed in concurrence as we scan over either the number of kicks or κ, while holding the other variable constant. We note from the figure that the concurrence values repeat after 25 kicks and $\kappa = 2\pi$. These plots capture the periodic nature of the dynamics of QKT with respect to both time and κ, which have been shown both analytically and experimentally in previous studies [42][70][11].

The time taken to obtain the experimental result from the quantum hardware runs was close to 2000 hours. We limited our experimental runs to 50 kicks per value of κ because of the following reason. In our experience the run time of the program scales linearly with the number of kicks. IBM delegates jobs to its processors depending on availability. A longer queue of the user's run requests leads to a longer run-time of the program. Since 50 kicks already cover two time periods of concurrence with respect to κ, we stopped after 2000 hours. One could run the program for longer and expect to obtain a repetition of the same pattern in concurrence.

2.7 Experimental Demonstration Beyond the Scope of Existing Experimental Techniques

The periodicity in concurrence, combined with our ability to simulate the dynamics for a high number of kicks, can be exploited to generate highly detailed average concurrence plots. By averaging over multiple periods of concurrence in the number of kicks, we reduced the estimation error of average concurrence.



(a) (b) (c)

Figure 2.6: (**a**). Stroboscopic phase space, (**b**) average concurrence over 200 kicks on IBMQ simulator and (**c**) average concurrence over 50 kicks on IBMQ-Vigo for 289 initial points and $\kappa = 2.5$.

A contour plot of concurrence against θ and ϕ for $\kappa = 2.5$ after averaging over 200 kicks on the simulator (Fig. 2.6b) and 50 kicks on the quantum hardware (Fig. 2.6b) bears a striking resemblance to the structure of stroboscopic phase space plot for the classical dynamics of the system at $\kappa = 2.5$. We observe that the chaotic regions of the classical phase space show intermediate concurrence values. The four prominently visible islands of low concurrence correspond to fixed points of the classical dynamics. These islands are clearly distinguishable even on the hardware plot and the left-right symmetry is maintained. Points $(J_x/j, J_y/j, J_z/j) = (1, 0, 0), (0, 0, -1), (-1, 0, 0)$ and $(1, 0, 0)$, which constitute a period-4 orbit present in the classical dynamics of the system, show the highest values of average concurrence.

We note the correspondence between this trend in average concurrence and the degree of delocalization of various initial states after evolution with the Floquet unitary. This degree of delocalization [43] can be quantified by calculating the maximum overlap with respect to the set of spin coherent states:

$$O_{\mathrm{SCS}}(|\psi(t)\rangle) = \max_{\mathrm{SCS}} |\langle \mathrm{SCS} \mid \psi(t)\rangle|. \tag{2.20}$$

Large values of O_{SCS} correspond to more localized states, as they indicate high overlap with spin coherent states. Delocalized states show low O_{SCS} values. The value of O_{SCS} for two different states, one in the low concurrence region ($(\theta, \phi) = (2.25, 1)$) and one in the high concurrence region ($(\theta, \phi) = (\pi/2, 0)$) have been plotted against number of kicks in Fig. 2.7.

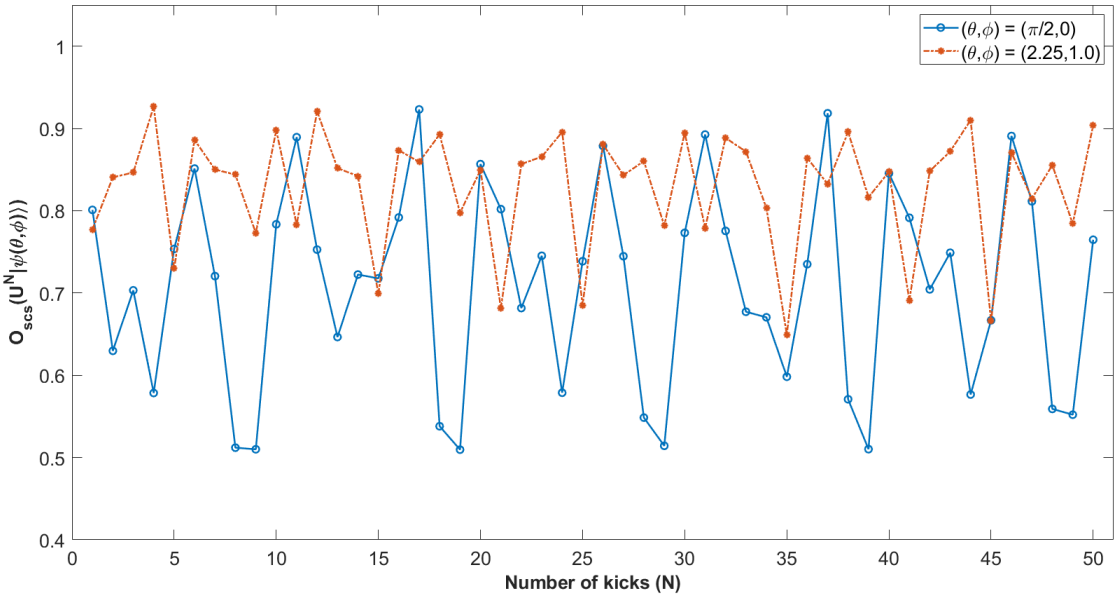


Figure 2.7: Evolution of O_{SCS} values for two different initial states. It is seen that the evolution of the initial point corresponding to more delocalized evolution ($(\theta, \phi) = (\pi/2, 0)$) has higher concurrence, i.e., has lower average O_{SCS} than that corresponding to less delocalized evolution ($(\theta, \phi) = (2.25, 1)$).

The results obtained in Fig 2.6c were predicted theoretically in many studies [42],[70],[53]. In 2016, Neill et al.[59] had obtained a similar structure in the experimental study for a three-qubit system using single-qubit entanglement entropy measures on a three-qubit ring of planar transmons with tunable inter-qubit coupling. Most of these studies have been done on systems with a large value of j, entering into the semi-classical regime. Here we show the correspondence in the deepest quantum system possible, i.e., a 2-qubit system.

To obtain this relationship between entanglement and chaos is remarkable, considering our system is in a deep quantum regime.

2.8 Efficient Simulation of the Quantum Kicked Top

It has been shown [71] that the theoretical lower bound of the number of CNOT gates required to simulate an arbitrary quantum gate acting on an n-qubit register is $(4^n - 3n - 1)/4$. To simulate a QKT with total angular momentum j, we need $2j$ qubits. Therefore, the minimum number of CNOT gates needed to simulate the QKT is given by $(4^{2j} - 6j - 1)/4$. In other words, the number of CNOT gates scales exponentially as a function of j. This makes the simulation of QKT unfeasible for high values of j. However, by utilizing the symmetry in the QKT Hamiltonian by which total angular momentum j is preserved, we propose an alternative approach to the quantum simulation of QKT.

For the QKT with total angular momentum operator J, $[H, J^2] = 0$. This means that J^2 is conserved, as a consequence of which any QKT state can be mapped into a state of $2j$ qubits with the constraint that it is permutation symmetric. The permutation symmetry reduces the dimensions of the $2j$ qubit Hilbert space from 2^{2j} to $2j + 1$. There exists an isomorphism from the system with total angular momentum j to the permutation symmetric subspace of $2j$ qubits.

Consider the Hilbert state of n qubits, $(\mathbb{C}^2)^{\otimes n}$. The computational basis states spanning the space is given by $|e_1\rangle \otimes |e_2\rangle \ldots |e_n\rangle$ where $e_i \in \{0, 1\}$. A symmetric subspace $\mathrm{Sym}^n(\mathbb{C}^2)$ of the n-qubit Hilber space is the set of all n-qubit states which are unchanged under the permutation of its qubits. $\mathrm{Sym}^n(\mathbb{C}^2) = \left\{ |\Phi\rangle \in (\mathbb{C}^2)^{\otimes n} : R_\pi |\Phi\rangle = |\Phi\rangle \right\}$ where R_π represents a permutation operation.

The Hilbert space of n qubits can be decomposed into the direct sum of symmetric subspaces.

$$\left(\mathbb{C}^2\right)^{\otimes n} \cong \mathrm{Sym}^{k_1}\left(\mathbb{C}^2\right) \oplus \mathrm{Sym}^{k_2}\left(\mathbb{C}^2\right) \oplus \ldots \oplus \mathrm{Sym}^{k_m}\left(\mathbb{C}^2\right) \quad k_1, \ldots, k_m \geq 0 \tag{2.21}$$

One of them should be $k_i = n$, the symmetric subspace $\mathrm{Sym}^n(\mathbb{C}^2) \subseteq (\mathbb{C}^2)^{\otimes n}$ of dimension $n + 1$, in which every QKT state of total angular momentum $j = n/2$ lies. Then the Floquet operator in the decomposed space may be expressed in the following block diagonal form:

$$U_{2^n} \cong \mathbb{I}_{2^n - (n+1)} \oplus U_{n+1} \tag{2.22}$$

where the subscripts represent dimension. This block diagonal form of the unitary Floquet operator can be decomposed into $O(\text{poly(n)})$ CNOT gates in contrast to $O(4^n)$ before the decomposition, since the nontrivial block has dimensions $(n+1)$ by $(n+1)$.

A unitary transformation on the computational basis states such that the resultant basis reflects the symmetries of the composite system present in the Hilbert space decomposition [Eq. (2.21)] can be done using the *quantum Schur transform* [4]. It is also efficient in the number of qubits (n), with a circuit complexity of $O(\text{poly(n)})$. It may be possible to use the quantum Schur transform to map the unitary Floquet operator (U_{2^n}) into the block diagonal form of Eq. (2.22). Assuming that it is possible, the combined circuit with the basis transformation using quantum Schur tansform and the application of Floquet operator can be brought down to $O(\text{poly(n)})$. However, the exact formulation of this procedure is still in progress and its success is yet to be determined.

To summarize, it may be possible to apply the quantum Schur transform to efficiently transform the computational basis states to a new basis in which the Floquet unitary of the n-qubit QKT can be efficiently decomposed into quantum gates for high n.

2.9 Summary and Outlook

In this chapter, we have proposed a quantum circuit-based approach to simulate and explore quantum chaos and demonstrated its advantages over existing methods. The proposed method can be applied in general to any periodically driven finite-dimensional quantum system. In our study, IBM's 5-qubit open access quantum chip (Vigo) was used as the experimental platform to implement the proposed approach for the 2-qubit quantum kicked top (QKT). The Hamiltonian of the QKT can be exactly expressed in terms of qubits since it is a finite-dimensional quantum system. Therefore, its evolution operator can be decomposed into quantum gates. Traditionally, experimental studies of quantum chaos have applied the same set of operations n times to explore time evolution. Here, we decomposed the unitary evolution operator for n kicks, U^n, into elementary quantum gates. This results in a fixed number of operations implementing the QKT evolution for any number of kicks. This hybrid combination of classical processing and quantum computing opens up the ability to perform high-fidelity experimental studies of quantum chaos in new parameter regimes.

Since the value of the chaoticity parameter κ only determines the parameters of unitary rotations in the quantum circuit, and since the single-qubit rotation errors are independent of the parameters, we were able to experimentally study chaotic dynamics over a wider

range of κ and kick number compared to previous studies. By taking advantage of the high fidelity obtained for both a large number of kicks and arbitrary κ values, we experimentally demonstrated the periodicity of entanglement with time and κ with high accuracy. Our studies also clearly showed signatures of chaos in the contour plot of average 2-qubit concurrence despite being in the deep quantum regime. Furthermore, we reported the first observation of the correspondence between average entanglement and delocalization in the 2-qubit QKT.

Our results demonstrate the advantages of circuit-based NISQ devices for exploring fundamental questions in quantum information and quantum chaos despite their noise and scale limitations. By applying error correction to the proposed circuit approach, our results could be improved even further. However, we leave this as future work.

The scheme used in this paper for the decomposition of an arbitrary unitary into elementary quantum gate requires exponentially many classical operations for higher values of j. This could make the realization of QKT consisting of several qubits computationally expensive. However, physical effects such as bifurcation are more pronounced in the QKT for higher j($\sim$ 100 qubits) [11]. To effectively observe bifurcation, it is necessary to use an efficient decomposition scheme. Indeed, there are certain symmetries in the floquet operator of the QKT which could allow a more efficient decomposition scheme. Exploring this possibility of efficient extension to a higher number of qubits is a natural next step of this work.

Chapter 3

Quantum Controlled Teleportation in the Presence of an Adversary

3.1 Introduction to Quantum Controlled Teleportation

Quantum teleportation is arguably one of the most important applications of entanglement. An arbitrary single-qubit state can be prepared at a remote location using an EPR state ($|\phi_\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}, \quad |\psi_\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$). Suppose Alice wants to teleport an arbitrary qubit state in her possession to Bob's location which is spatially separated. Alice and Bob share an EPR state in the past before separating. Alice performs a two-qubit measurement in the Bell basis on the state to be teleported and her share of the EPR state. She sends the outcome of her two-qubit measurement to Bob. Depending on which EPR state was shared between them and the outcome of Alice's measurement, Bob performs a unitary rotation on his share of the two-qubit EPR state to recover the arbitrary qubit state that was earlier in Alice's possession. In this process, the quantum information stored by Alice in the arbitrary qubit is transferred to Bob.

First introduced in 1993 [9], quantum teleportation and its relationship with nonlocality and entanglement has been studied extensively [65][37][14],[39]. Experimental demonstrations [64] including long distance and ground-satellite teleportation [83][68] have been achieved.

Multipartite generalizations of quantum entanglement such as controlled quantum teleportation (CQT) play an important role in Quantum Teleportation Networks. In such a

network, entanglement is shared between more than two parties. In the tripartite case, teleportation can be performed between any two parties but only with the help of the third party [84]. These networks are an integral part of the hypothetical quantum internet [13]. CQT finds direct application in the well-known quantum secret sharing protocol [36] where information is distributed among multiple parties and no single party is sufficient to reconstruct the whole information. In the simplest CQT scenario, a GHZ state of the form $(|000\rangle + |111\rangle)/\sqrt{2}$ is shared between three parties: Alice, Bob and Charlie. Suppose Alice wants to teleport a qubit to Bob. For faithful teleportation, Charlie needs to perform a measurement in the σ_X basis such that Alice and Bob's bipartite state is projected into $|\phi_\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ depending on the measurement outcome. Charlie reveals his measurement outcome to Alice and Bob. Then they perform the usual two-qubit teleportation since they now know which EPR pair (i.e., $|\phi_+\rangle$ or $|\phi_-\rangle$) is being shared between them. Without knowing Charlie's measurement outcome, the maximum fidelity of teleportation averaged over all possible arbitrary qubit states is 2/3. It has been shown that the maximum average fidelity of teleportation using only classical resources where a single input state is measured at Alice's site, and the result of the measurement is sent over a classical channel to Bob (who reconstructs the state) is 2/3 [40]. In a valid CQT protocol, the teleportation cannot be performed with an average fidelity $> 2/3$ without Charlie's permission. Thus, Charlie plays the role of a controller by which he decides whether Alice and Bob should use quantum resources for teleportation. There have been several attempts to experimentally implement the CQT protocol [84][60][83][82][7]. To my knowledge, the most successful of them was Barasinski et al. (2019) [7] where discrete variable linear optics was used. They achieved an experimental fidelity of 83.0 ± 0.7 with Charlie's permission and 51.8 ± 6.7 without Charlie's permission.

Often, the devices used for performing quantum communication/ cryptographic protocols such as quantum teleportation and CQT are manufactured and supplied by external agents. The inner working of the devices could be hidden from the users. The black box or device independent (used interchangeably in the rest of the chapter) approach is useful for testing whether a given device functions according to its specifications. In 2013, Bancal et al. [38] have studied in the black box scenario whether quantum resources are being used for the standard teleportation of a qubit. To our knowledge, there is no device independent study of the CQT scheme. In this thesis, we go one step further and study the device independent scenario of a more practical version of the CQT involving three parties -controller, sender and receiver- where the receiver is untrusted. We ask the following questions:

- How to device independently test whether quantum resources are being used for the controlled teleportation of a qubit with an untrusted receiver?

- Sometimes, the device will use quantum resources and still be far away from its ideal functionality. What happens to the controller's authority if the untrusted receiver attempts to perform the teleportation by taking advantage of the non-ideal quantum device even when the controller has not allowed?

- Can we predict the level of controller's authority by device independently testing a device which allegedly performs controlled quantum teleportation given that the receiver is untrusted?

First we will introduce the standard quantum teleportation protocol [9] and the standard CQT protocol [40] in Sections 3.2.1 and 3.2.2 respectively. Then we will review the device independent teleportation of a qubit in Section 3.2.3, which will lead to our construction of the device independent *controlled* teleportation of a qubit with an untrusted receiver in Section 3.3. We will present our quantification of the controller's authority in CQT with a non-ideal device in Section 3.4. Finally, we will present two examples to demonstrate the quantitative nature of the controller's authority with respect to a device-independently testable quantity in Section 3.4.2.

3.2 Background

3.2.1 Quantum Teleportation

We will review the standard quantum teleportation protocol in more detail in this section. The objective of this protocol is to teleport an unknown pure qubit ($\rho^a = \frac{\mathbb{I}_2+\vec{a}.\vec{\sigma}}{2}$) in the possession of Alice to Bob.

- Alice and Bob share a maximally entangled state $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

- Alice performs a Bell state measurement on her qubit of $|\Phi^+\rangle$ and the unknown qubit ρ^a. The set of outcomes is given by $c_0c_1 \in \{00, 01, 10, 11\}$. After Alice's measurement, Bob's qubit takes the form $\rho^B_{c_0c_1} = \frac{\mathbb{I}_2+(R_{c_0c_1}\vec{a}).\vec{\sigma}}{2}$

- Alice communicates the outcome of her Bell measurement to Bob via a classical channel.

- Bob performs the corrective rotation $R^{-1}_{c_0c_1}$ to prepare the unknown state ρ^a in his qubit.

3.2.2 Control Power in CQT

The controlled quantum teleportation protocol is similar to the standard quantum teleportation protocol with an added step. The objective is to teleport an unknown qubit in the possession of Alice to Bob only with the participation of Charlie.

1. Let Alice, Bob and Charlie share a GHZ state of the form $(|000\rangle_{ABC}+|111\rangle_{ABC})/\sqrt{2}$. It can be equivalently expressed as $(|\phi^+\rangle_{AB}|+\rangle_C+|\phi^-\rangle_{AB}|-\rangle_C)/\sqrt{2}$. Henceforth, the subscripts A, B, C will be dropped.

2. Charlie performs a projective measurement in the σ_X basis and gets an outcome $\gamma \in \{\pm 1\}$. His measurement operators are given by:

$$M_C^\gamma = \frac{(\mathbb{I}_2 + \gamma\sigma_X)}{2}; \qquad \gamma \in \{\pm 1\} \tag{3.1}$$

   After Charlie's measurement, Alice and Bob's joint state is given by the following:

$$\rho_\gamma^{AB} = tr^C(\rho_{GHZ}.(\mathbb{I}\otimes\mathbb{I}\otimes M_C^\gamma)) \tag{3.2}$$
$$= |\phi^\gamma\rangle\langle\phi^\gamma| \tag{3.3}$$

3. Let the arbitrary state to be teleported be given by:

$$\rho^a = \frac{\mathbb{I}_2 + \vec{a}.\vec{\sigma}}{2} \tag{3.4}$$

   Alice performs a Bell state measurement on the first two qubits of the state $\rho^a \otimes \rho_\gamma^{AB}$. the Bell state measurement is given by the following measurement operators:

$$M_{c_0c_1}^A = |\phi^{c_0c_1}\rangle\langle\phi^{c_0c_1}| \tag{3.5}$$

   where

$$|\phi^{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}; |\phi^{01}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}; |\phi^{10}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}; |\phi^{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

   After Alice's measurement, Bob's state is projected into the following state:

$$\rho_{c_0c_1}^B = \frac{\mathbb{I}_2 + (R_{c_0c_1\gamma}\vec{a}).\vec{\sigma}}{2} \tag{3.6}$$

   where

$$\begin{aligned} &R_{0,0,+1} = R_z(\pi); R_{0,1,+1} = \mathbb{I}_2; R_{1,0,+1} = R_z(\pi); R_{1,1,+1} = R_z(\pi) \\ &R_{0,0,-1} = \mathbb{I}_2; R_{0,1,-1} = R_z(\pi); R_{1,0,-1} = R_x(\pi); R_{1,1,-1} = R_y(\pi) \end{aligned} \tag{3.7}$$

4. Now Bob performs an $R^{-1}_{c_0c_1\gamma}$ rotation to retrieve ρ^a.

$$\rho^B = \frac{\mathbb{I}_2 + (R^{-1}_{c_0c_1\gamma}.R_{c_0c_1\gamma}\vec{a}).\vec{\sigma}}{2} = \frac{\mathbb{I}_2 + \vec{a}.\vec{\sigma}}{2} = \rho^a \tag{3.8}$$

The average fidelity of teleportation between the unknown pure state (ρ^a) and Bob's final state (ρ^B) is given by

$$F = \int \frac{d\vec{a}}{4\pi} \langle a| \rho^B |a\rangle \tag{3.9}$$

where the averaging has been performed over all pure qubit states. Henceforth, we will refer to the average fidelity of teleportation performed with Charlie's participation as F_C and that without Charlie's participation as F_{NC}. From Eq. (3.8) and Eq. (3.9),

$$F_C = \int \frac{d\vec{a}}{4\pi} \langle a| \frac{\mathbb{I}_2 + \vec{a}.\vec{\sigma}}{2} |a\rangle = 1 \tag{3.10}$$

Suppose Charlie does not reveal γ. Bob will randomly perform either $R^{-1}_{c_0c_1,+1}$ or $R^{-1}_{c_0c_1,-1}$. In that case, the average teleportation fidelity is given by:

$$F_{NC} = \int \frac{d\vec{a}}{4\pi} \sum_{\gamma,\gamma'\in\{1,-1\}} \sum_{c_0,c_1\in\{0,1\}} P(\gamma,\gamma',c_0,c_1) \langle a| \frac{\mathbb{I}_2 + (R^{-1}_{c_0c_1\gamma}.R_{c_0c_1\gamma}\vec{a}).\vec{\sigma}}{2} |a\rangle \tag{3.11}$$

where $P(\gamma,\gamma',c_0,c_1) = P(c_0,c_1|\gamma,\gamma')P(\gamma,\gamma')$; $P(\gamma,\gamma') = P(\gamma|\gamma')P(\gamma')$

$$P(\gamma') = \mathrm{tr}(\rho_{GHZ}.(\mathbb{I}\otimes\mathbb{I}\otimes M_C^{\gamma'})) = \frac{1}{2} \tag{3.12}$$

$$P(\gamma|\gamma') = P(\gamma') = \frac{1}{2} \tag{3.13}$$

therefore,

$$P(\gamma,\gamma') = \frac{1}{2}.\frac{1}{2} = \frac{1}{4} \tag{3.14}$$

$$P(c_0,c_1|\gamma,\gamma') = \mathrm{tr}(\rho^{AB}_\gamma M^A_{c_0c_1}) = \frac{1}{4} \tag{3.15}$$

Substituting the above conditional probabilities in Eq. (3.11), we get

$$F_{NC} = \int \frac{d\vec{a}}{4\pi} \sum_{\gamma,\gamma'\in\{1,-1\}} \sum_{c_0,c_1\in\{0,1\}} \frac{1}{16} \langle a| \frac{\mathbb{I}_2 + (R^{-1}_{c_0c_1\gamma}.R_{c_0c_1\gamma}\vec{a}).\vec{\sigma}}{2} |a\rangle = \frac{2}{3} \tag{3.16}$$

The control power of Charlie is given by the difference between F_C and F_{NC}. The intuition is that without the controller's participation, the average teleportation fidelity must be minimized and that with the controller's participation must be maximized. Thus, higher the difference between the above fidelities, higher is the control [49]. The control power of Charlie is expressed as follows:

$$CP = F_C - F_{NC} = 1 - \frac{2}{3} = \frac{1}{3} \tag{3.17}$$

3.2.3 Device Independent Certification of Quantum Resources Used in Teleportation

In the usual two-party teleportation protocol using EPR states, Bancal et al. [38] suggested a construction by which it is possible to certify whether a teleportation device is using quantum resources. Alice and Bob have been given a pair of black boxes that supposedly perform the quantum teleportation of a qubit state. The input of each box is a unit vector of the Bloch sphere. Alice's box takes the state to be teleported as the input given by the vector $\vec{a}$ and outputs two bits $(c_0c_1) \in \{0,1\}^2$. Bob's box takes a vector $\vec{b}$ as input and gives one bit output $\beta \in \{+1,-1\}$. $\vec{b}$ represents a measurement of the teleported state in the $\vec{b}.\vec{\sigma}$ direction. The vendor claims that their boxes contain EPR states, using which the teleportation is performed on each run. Alice and Bob wish to verify the vendor's claim.

In [38], it was shown that it is indeed possible to certify teleportation in this black box scenario. In other words, it is possible to infer a posteriori that the black boxes used quantum resources to perform the teleportation from the input/output statistics of the boxes.

In a teleportation protocol, Alice is typically required to send (c_0, c_1) to Bob such that he can perform the appropriate corrective rotation based on some pre-established agreement to prepare the unknown qubit. However, it was shown [75] that 2 classical bits of information are enough to simulate the statistical correlations of the maximally entangled singlet state. Hence, a black box certification of quantum resources is not possible if Alice communicates with Bob. Therefore, Alice and Bob do not reveal any of their measurement input/output until several (ideally infinite) rounds have been completed. Each round consists of the pair of boxes taking inputs $(\vec{a}, \vec{b})$ and giving outputs (c_0c_1, β). In the end, they can construct the probability distributions $P(c_0c_1, \beta|\vec{a}, \vec{b})$. Alice and Bob have no knowledge of the inner working of the composite black boxes except that they are not communicating. It is also assumed that Alice and Bob have free will. At the end of the protocol, the only information they have is the data table of inputs and outputs $(c_0c_1, \beta|\vec{a}, \vec{b})$ for each round. Using this,

they must test whether the source of correlations is quantum. This scenario can be easily mapped into a Bell scenario.

Let Alice choose from state settings $\{\vec{a_1}, \vec{a_2}\}$ and Bob choose from measurement setting $\{\vec{b_1}, \vec{b_2}\}$. Alice's black box gives two bits (c_0, c_1) as the output, which must be mapped to one bit. This can be done by choosing $\alpha = 2c_j - 1$ if Alice's input is a_j. Thus, one can construct the distributions $P(\alpha, \beta|j, k)$ from $P(c_0c_1, \beta|\vec{a}, \vec{b})$. Finally, the Clauser-Horne-Shimony-Holt (CHSH) Bell function can be calculated as:

$$CHSH = \sum_{j,k\in\{0,1\}} P(\alpha = \beta|j, k) - P(\alpha \neq \beta|j, k) \tag{3.18}$$

If $CHSH > 2$, it is guaranteed that the pair of black boxes generate statistical correlations that are not possible to generate using only classical resources [8]. In other words, if $CHSH > 2$, it is certified that quantum resources are being used for teleportation.

3.3 Device Independent Controlled Teleportation of a Qubit to an Untrusted Receiver

Here we consider a controlled teleportation scenario where a qubit in the possession of Alice (sender) is teleported to Bob (receiver) only when Charlie (controller) participates. However, Bob is not a trusted party. Bob can collude with external agents henceforth labelled Derek to extract extra information that can increase the fidelity of teleportation even without Charlie's participation. An untrusted receiver can therefore lead to a decrease in the control power of Charlie. In this section, our goal is to certify the controller's authority of Charlie in such a scenario. The goal of a CQT protocol is to ensure that Charlie can control whether quantum resources are being used for teleportation. Hence it is necessary to first certify that the given device is capable of using quantum resources for teleportation. We will present a construction using which it is possible to certify whether quantum resources are being used for controlled teleportation to an untrusted receiver.

3.3.1 A Test of Quantum Resources in CQT with Untrusted Receiver

The idea of certification of quantum resources used in black box teleportation described in Section 3.2.3 can be adapted for black box *controlled* teleportation.

3.3.2 Scenario

Derek supplies three black boxes to Alice, Bob and Charlie which can allegedly perform controlled quantum teleportation of a qubit such that Charlie is the controller, Alice is the sender and Bob is the receiver. The ideal functions of the three black boxes are as follows:

1. Charlie's black box: Accepts a measurement setting $\vec{c} \in S^2$ as input and upon measurement gives an outcome $\gamma \in \{0, 1\}$.
2. Alice's black box: Accepts the state to be teleported $\vec{a} \in S^2$ as input and upon Bell-measurement [Eq. (3.5)] gives an outcome $s_0 s_1 \in \{0, 1\}^2$.
3. Bob's black box: Performs a corrective rotation $R^{-1}_{s_0 s_1 \vec{c} \gamma}$ which is specified in the instruction manual of the device. Accepts a measurement setting $\vec{b} \in S^2$ as input and upon measurement gives an outcome $\beta \in \{0, 1\}$.

In an ideal CQT scheme, the shared state of Alice, Bob and Charlie's black boxes is the GHZ state $(|000\rangle + |111\rangle)/\sqrt{2}$. The analysis of this ideal scheme has been shown in Section 3.2.2. The control power of Charlie for the ideal CQT scheme is $CP = \frac{1}{3}$.

However, we do not assume anything apriori regarding the inner working of the black boxes - including the underlying composite state of Alice, bob and Charlie and their individual measurement basis. Additionally, we do not trust the receiver Bob. Therefore, Alice and Charlie are *trusted* and Bob is *untrusted*.

3.3.3 The Adversary

In the above scenario 3.3.2, let Bob be the *untrusted* part and Derek be the *eavesdropper*. Together, they play the role of an *adversary*.

Adversarial Goal

The goal of the adversary is to maximize the average teleportation fidelity when Charlie has not allowed the teleportation i.e., not revealed the input setting $\vec{c}$ and the outcome γ of his measurement.

Adversarial Capabilities

1. The eavesdropper Derek is restricted to acting on individual signals separately.
2. Derek can generate the shared states of the black boxes i.e., hold the common source of correlations but has no direct access to the input/output variables of the three parties.
3. The untrusted party Bob can correlate his inputs with that of the common source of correlations held by Derek.
4. Derek and Bob can jointly extract another outcome δ that can be potentially used to increase the fidelity of teleportation. This means that the corrective rotation performed by Bob can also depend on δ. This extra capability of the adversary allows us to write Bob's corrective rotations as $R^{-1}_{s_0 s_1 \vec{c} \gamma \delta}$ in contrast to $R^{-1}_{s_0 s_1 \vec{c} \gamma}$ in the ideal scenario.

3.3.4 Device Independent Test of Quantum Resources

Consider a restriction to the ideal scenario described in Section 3.3.2:

Device Independent Test Scenario

1. Derek is the manufacturer and supplier of the black boxes of Alice, Bob and Charlie.
2. Alice, Bob and Charlie's black boxes cannot communicate with each other.
3. Charlie's black box: Accepts a measurement setting out of two distinct choices $\vec{c} \in \{\vec{c_0}, \vec{c_1}\}$ as input and upon measurement gives an outcome $\gamma \in \{0, 1\}$.
4. Alice's black box: Accepts the state to be teleported out of two distinct states $\vec{a} \in \{\vec{a_0}, \vec{a_1}\}$ as input and upon Bell-measurement [Eq. (3.5)] gives an outcome $s_0 s_1 \in \{0, 1\}^2$.
5. Bob's black box: Performs a corrective rotation R^{-1}_{δ} given to him by Derek. Accepts a measurement setting out of two distinct choices $\vec{b'} \in \{\vec{b'_0}, \vec{b'_1}\}$ as input and upon measurement gives an outcome $\beta \in \{0, 1\}$. Equivalently, the corrective rotation can be included in the measurement of Bob such that the new measurement choices are $\vec{b} = \{\vec{b_0} = R^{-1}_{\delta} \vec{b'_0}, \quad \vec{b_1} = R^{-1}_{\delta} \vec{b'_1}\}$.

6. Alice and Charlie independently choose their individual measurement setting i.e., their choice of measurement setting depends only on their free-will. However, Bob's choice of measurement setting can be influenced by Derek. Therefore, the untrusted receiver does not have free-will.

7. We require that the announcement of inputs and measurement outcomes be made simultaneously by all parties after several rounds of the experiment have been completed. This ensures that the inputs or outcomes of the trusted parties are not used to the advantage of the untrusted part.

8. The announcements at the end of several rounds of sending in inputs and recording outcomes from each black box will be a table of $(s_0 s_1, \beta, \gamma)$ given (i, j, k) for each round where i, j, k denote the input setting (0 or 1) of Alice, Bob and Charlie respectively. From this data, the joint probability distribution $p(s_0 s_1, \beta, \gamma | i, j, k)$ can be computed.

For the purpose of device independent testing, we require that Alice's output i.e, $s_0 s_1$ be mapped into a single bit α in the following way:

$$\alpha = 2s_j - 1 \quad \text{where Alice's input is } \vec{a_j}$$

Using this map, one can construct the distributions $P(\alpha, \beta, \gamma | j, k, l)$ from $P(s_0 s_1, \beta, \gamma | \vec{a}, \vec{b}, \vec{c})$.

Remark 1. *The choice of input merely indicates that each party can choose to press one out of two buttons. It is assumed that the parties do not know which measurement basis the buttons correspond to.*

Causal Structure of the Device Independent Test Scenario

The causal structure of inputs, outcomes and common source of correlations of the different parties involved can be represented in the following way using directed acyclic graphs (DAG):

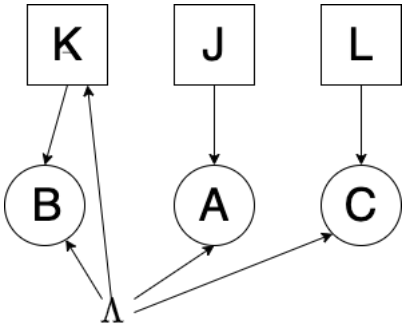


Figure 3.1: DAG representation of the causal model where Λ is the common source of correlations supplied by Derek. In a classical model, Λ is a shared random variable whereas in a quantum model, Λ is a potentially entangled quantum state ρ. Here J, K, L denote the inputs of Alice, Bob and Charlie respectively. A, B, C denote the outcomes of Alice, Bob and Charlie respectively. Note that, since Bob is untrusted, he can correlate his inputs with that of the common source of correlations.

In Fig. 3.1, each directed edge represents a causal relation between two nodes. The start of each edge is called the parent node and the arrival of each edge is called the child node. In a classical causal model, the source of correlations and all other nodes are random variables such that the parent nodes completely characterize a child node.

The explanation of how to interpret the DAG in Fig. 3.1, is as follows:

- The node Λ represents the common source of correlations (the underlying state in the black boxes) supplied by the eavesdropper Derek himself.
- J, K, L denote the inputs (measurement choices) of Alice, Bob and Charlie respectively. A, B, C denote the outcomes α, β, γ of Alice, Bob and Charlie respectively.
- The arrows from Λ to A, B and C represent the fact that the outputs of Alice, Bob and Charlie depend on the underlying state of their black boxes.
- The arrows from J, K, L to A, B, C respectively represent the dependence of the outcomes of each party on the choice of their measurement setting.
- There are no arrows from the input or outcome of one party to another because their black boxes are not allowed to communicate with each other (Section 3.3.4).

- Since the inputs of the trusted parties Alice and Charlie can be independently chosen (measurement setting choice independence/free-will), J and L have no parent nodes.
- Since Bob is untrusted, his input may be correlated with that of the common source of correlations. Hence, Bob does not have measurement independence. The arrow from Λ to K represents the fact that Bob's choice of measurement setting depends on the information he receives from Derek through the black box.
- Extra arrows from inputs/outcomes from one party to another could be avoided due to the requirement that all announcements be made simultaneously at the end of several rounds.

If $\{v_i\}_{i=1}^n$ denote the nodes of the graph, $p(v_k|v_1, v_2, ..., v_n) = p(v_k|pa(v_k))$ where $pa(v_k)$ denotes all parent nodes of v_k. Thus, the joint probability distribution of all the nodes is given by $p(v_1, v_2, ..., v_n) = \Pi_{v_i} p(v_i|pa(v_i))$.

Therefore, in the causal structure with an untrusted receiver (Fig. 3.1), if Λ is a classical random variable then the joint probabilities must admit the following decomposition:

$$p(\alpha\beta\gamma\delta|ijk) = \sum_{\lambda} p(\alpha|j\lambda)p(\beta|k\lambda)p(\gamma|l\lambda)p(\delta|k\lambda)p(\lambda|k) \tag{3.19}$$

Bell Inequality Characterizing the Device Independent Test Scenario

In [16] it was shown that the following DAGs are equivalent:

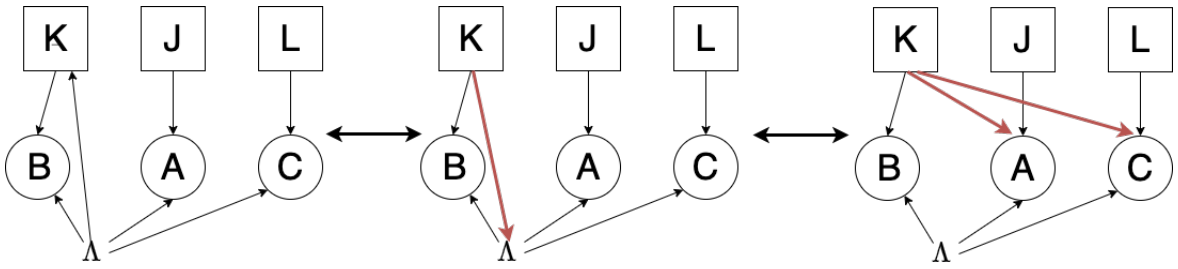


Figure 3.2: DAG Equivalence

This means that the DAG representing the device independent scenario of controlled teleportation with an untrusted receiver (left-most DAG) is equivalent to the broadcasting

scenario (right-most DAG). Broadcasting represents a scenario where one or more parties can openly communicate their choice of input to other parties. Here, in the right-most DAG it is seen that Bob communicates his choice of input to Alice and Charlie.

In [6], the Bell inequalities characterizing the broadcasting scenario were studied. In the case of n parties out of which $n-m$ parties broadcast their inputs to all other parties and the remaining m parties do not communicate their input to any other party, the tight bound to a specific Bell inequality called the Svetlichny inequality was found.

The Svetlichny function involves distributions of the form $p(\alpha\beta\gamma|ijk)$ which is obtained from the device independent test rounds.

$$\begin{aligned} S =& p_A(+1 \mid 0)\mathrm{CHSH}_{(+1)0} - p_A(-1 \mid 0)\mathrm{CHSH}_{(-1)0} \\ &+ p_A(+1 \mid 1)\mathrm{CHSH}'_{(+1)1} - p_A(-1 \mid 1)\mathrm{CHSH}'_{(-1)1} \end{aligned} \tag{3.20}$$

where $p_A(\alpha \mid j)$ is the marginal probability of Alice, $\mathrm{CHSH}_{\alpha j}$ and $\mathrm{CHSH}'_{\alpha j}$ refer to symmetries of the Clauser-Horne-Shimony-Holt (CHSH) inequality given by $\mathrm{CHSH}= E^{\alpha j}_{(+1)0} + E^{\alpha j}_{(+1)1} + E^{\alpha j}_{(-1)0} - E^{\alpha j}_{(-1)1}$ and $\mathrm{CHSH}'_{\alpha j} = E^{\alpha j}_{(+1)0} - E^{\alpha j}_{(+1)1} - E^{aj}_{(-1)0} - E^{\alpha j}_{(-1)1}$, and $E^{\alpha j}_{yz} = \sum_{\beta,\gamma=+1,-1} \beta\gamma\ p(\beta,\gamma \mid j,\alpha,k,l)$ is the expectation value of the measurement outcome of Bob and Charlie conditioned on a given outcome α and the input j of Alice.

The result from ref. [6] that we will use in this chapter is given by the following statement:

For the broadcasting scenario where $n-m$ is odd, $|S| \leq 2^{(n-m)/2+3/2}$. Moreover, this bound is tight, i.e., there exists a classical strategy (Λ) such that $|S| = 2^{(n-m)+3/2}$.

In the broadcasting scenario of our interest (right-most DAG in Fig. 3.2), $n = 3$ and $m - n = 1$. Therefore, in this case,

$$|S| \leq 4 \tag{3.21}$$

Using this result [Eq. (3.21)] and the equivalence of DAGs (Fig. 3.2), we can immediate make the following claim:

Claim 1. *Any probability distribution $p(\alpha\beta\gamma|ijk)$ admitted by the DAG representing the device independent test scenario of controlled quantum teleportation with an untrusted receiver (as defined in Section 3.3.4) using classical strategies must satisfy the Svetlichny inequality $|S| \leq 4$. Moreover, this bound is tight.*

Condition for certification of quantum resources: If the Svetlichny inequality $|S| \leq 4$ is violated, it is guaranteed that the observed probability distribution $p(\alpha\beta\gamma|ijk)$

was not generated entirely by classical means. Hence, the source of correlations (Λ) must be quantum.

Comparison with the Device Independent Scenario of Fully Trusted Controlled Quantum Teleportation

In controlled quantum teleportation where all parties are trusted, it is easy to see that the device independent test scenario is represented by the following DAG:

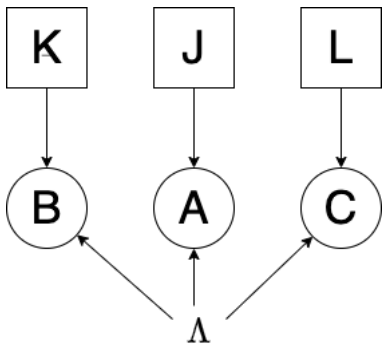


Figure 3.3: DAG for the device independent test scenario of fully trusted controlled quantum teleportation. Note that there are no arrows from Λ to K unlike that in the scenario of untrusted receiver considered earlier. Here, all parties have measurement choice independence and there is no communication between each other.

This device independent scenario is certified to be quantum if the obtained correlations violate Mermin's inequality [57]. A maximal violation of Mermin's inequality implies that the underlying state is the GHZ state, therefore guaranteeing maximum control power. However, it was shown in Ref. [58] that there exists a local model in the broadcasting scenario of Fig. 3.2, that violates Mermin's inequality maximally. Since the device independent scenario of controlled teleportation with an untrusted receiver is equivalent to the broadcasting scenario (Fig. 3.2), Mermin's inequality is not sufficient for its certification.

The presence of an untrusted part makes it necessary to use a stronger notion of nonlocality also known as genuine tripartite nonlocality/Svetlichny nonlocality for the certification of controlled teleportation.

When is the Controller's Authority Maximum?

Claim 2. *Controller's authority is maximum with* $CP = \frac{1}{3}$ *in the controlled quantum teleportation scheme if* $S = 4\sqrt{2}$ *is obtained from the device independent test.*

Proof. Because of the normalization of $p_A(a \mid x)$, to achieve the maximum quantum violation $S = 4\sqrt{2}$ necessarily, we must have $\text{CHSH}_{(-1)0} = \text{CHSH}'_{(-1)1} = -2\sqrt{2}$ and $\text{CHSH}_{(+1)0} = \text{CHSH}'_{(+1)1} = 2\sqrt{2}$. For any given α and j, Charlie and Bob's joint state must maximally violate the CHSH. Only maximally entangled two-qubit pure states can generate such a correlation.

Thus, by the monogamy of entanglement, $\rho^{BCD} = \rho^{BC} \otimes \rho^{D}$ where ρ^{BC} is a maximally entangled pure state of Bob and Charlie. This means that if $S = 4\sqrt{2}$, then Derek cannot remain entangled to Bob and Charlie's devices.

Now suppose the same device which yielded $S = 4\sqrt{2}$ during the device independent test, is used for the standard controlled quantum teleportation scheme (Section 3.2.2). If Charlie does not give permission to teleport i.e., does not reveal γl then $p(\delta = \gamma l) = \frac{1}{4}$. This reflects the fact that Derek's state is separate from Bob and Charlie's composite state and therefore cannot obtain information about their systems by performing local operations on his system. Essentially, it means that Bob has no extra information about what the corrective rotations $R^{-1}_{s_0 s_1 \gamma l}$ are beyond what the trusted parties Alice and Charlie choose to reveal.

Alternatively, we note that only the maximally entangled GHZ state $\frac{|000\rangle + |111\rangle}{2}$ (upto local unitary operations) violates the Svetlichny inequality maximally, i.e., gives $S = 4\sqrt{2}$. It directly follows that Derek's state must be separated from the tripartite state of Alice, Bob and Charlie since the maximally entangled GHZ state is a pure quantum state. The controller's authority for the GHZ state was derived in Section 3.2.2 and CP was shown to be 1/3. □

3.4 Controller's Authority from Non-maximal Violation of Svetlichny Inequality

In Section 3.2.3, we constructed an experiment by which the Svetlichny function can be computed. We showed that a maximal violation of the Svetlichny Inequality [Eq. (3.21)] implies that Bob can get no useful information from Derek to increase the average teleportation fidelity without Charlie's permission. This ensures that the controller's authority is

maximized. However, one can expect that controller's authority will not be maximized in case of non-maximal violation of the Svetlichny Inequality.

Having solved the general task of certifying whether the black box device which allegedly performs controlled quantum teleportation, is actually using quantum resources, we will take the example of two specific families of quantum states to study the quantitative relationship of genuine 3-way nonlocality with controller's authority. In this section, we will consider two noise models of the tripartite GHZ state - the total depolarizing channel and the qubit depolarizing channel - and compute the controller's authority as a function of Svetlichny Inequality [Eq. (3.21)] violation. We will consider a specific attack strategy using which Bob will try to increase the average fidelity of teleportation without Charlie's permission. Charlie's authority will be quantified by the Effective Control Power (ECP) which we define as

$$ECP = F_C^{NE} - F_{NC}^{E} \tag{3.22}$$

Here F_C^{NE} indicates the average fidelity of teleportation with Charlie's permission and no eavesdropping. F_{NC}^{E} indicates the average fidelity of teleportation without Charlie's permission but with eavesdropping (i.e., Derek's participation). The general definition of controller's authority would be

$$CP = F_C^{E} - F_{NC}^{E} \tag{3.23}$$

The superscripts (E) indicate that eavesdropping has been considered in both cases of control i.e., with and without Charlie's permission. We shall leave the more general quantification of controller's authority as future work and focus on Effective Control Power (ECP) of Charlie in this section. Note that $F_C^{E} \geq F_C^{NE}$ because eavesdropping will always increase fidelity. Therefore, ECP is a lower bound to the more general definition of controller's authority quantified by [Eq. (3.23)]. It is guaranteed that for the adversarial strategy under consideration, Charlie has at least ECP amount of control.

3.4.1 Adversarial Strategy

The ideal CQT scheme (Section 3.2.2) using the tripartite GHZ state allows teleportation with perfect average fidelity with Charlie's permission. Alice and Bob's composite state is projected into one of the EPR states after Charlie performs a measurement on her system and reveals the measurement setting and outcome to Bob. When Charlie does not make his measurement information known to Bob i.e., does not give permission to teleport, Bob does not know which EPR state the teleportation channel has been projected into. This prevents Bob from achieving an average teleportation fidelity higher than 2/3 without Charlie's permission. Recall that the goal of the adversary (Section 3.3.3) is to maximize

the average teleportation fidelity when Charlie has not allowed the teleportation. Bob's next best option is to ask Derek to perform a measurement in a suitable basis and reveal its outcome (δ) to Bob such that Alice and Bob's composite state is projected close to one of the four EPR states. This gives Bob some relevant information regarding the corrective rotations using which he can recover the state to be teleported with higher fidelity (see point 4 of Adversarial Capabilities, Section 3.3.3). Our goal is to find the maximum fidelity of teleportation that Bob can achieve without permission from Charlie using this extra information (δ), which is required to evaluate the worst case Effective Control Power (ECP) of Charlie.

Thus, the adversarial strategy can be formulated as the following problem:

Proposition 1. *Adversarial strategy: Find the optimal POVM operators (Appendix A) of Derek such that the fidelity between the post-measurement state of Alice and Bob conditioned on Derek's measurement outcome and one of the EPR states is maximized.*

Execution of Adversarial Strategy

The adversarial strategy in Proposition 1 can be executed in the following way:

Let $\{M_i\}$ denote Derek's POVMs, and $Pr(i)$ denote the probability of getting an outcome i. ρ^{ABD} is the joint state of Alice, Bob and Derek. Note that Charlie's state is irrelevant in this case since he is not participating.

Then the post measurement state of Alice and Bob is given by

$$\rho_i^{AB} = \frac{\mathrm{Tr}^D(\rho^{ABD}\mathbb{I}\otimes\mathbb{I}\otimes M_i)}{Pr(i)} \tag{3.24}$$

Let $F(\rho_1,\rho_2)$ denote the fidelity between two density matrices ρ_1 and ρ_2. Then the problem of finding the optimal POVMs can be formulated as follows:

$$\begin{aligned} &\text{Maximize} && \sum_i Pr(i)F(\rho_i^{AB}, |\phi_i\rangle\langle\phi_i|) \\ &\text{Subject To} && M_i \geq 0,\ \sum_i M_i = \mathbb{I} \end{aligned} \tag{3.25}$$

$$\begin{aligned} Pr(i)F(\rho_i^{AB}, |\phi_i\rangle\langle\phi_i|) &= \mathrm{Tr}\big(\mathrm{Tr}^D(\rho^{ABD}\mathbb{I}\otimes\mathbb{I}\otimes M_i)\,|\phi_i\rangle\langle\phi_i|\big) \\ &= \mathrm{Tr}\big((|\phi_i\rangle\langle\phi_i|\otimes\mathbb{I})\rho^{ABD}(\mathbb{I}\otimes\mathbb{I}\otimes M_i)\big) \\ &= \mathrm{Tr}\big(\mathrm{Tr}^D((|\phi_i\rangle\langle\phi_i|\otimes\mathbb{I})\rho^{ABD})M_i\big) \end{aligned} \tag{3.26}$$

Let $\tilde{\rho}_i = \mathrm{Tr}^D((|\phi_i\rangle\langle\phi_i| \otimes \mathbb{I})\rho^{ABD})$. After substituting $\tilde{\rho}$ in Eq. (3.25), we get:

$$\begin{aligned} &\text{Maximize} && \sum_i \mathrm{Tr}(\tilde{\rho}_i M_i) \\ &\text{Subject To} && M_i \geq 0,\ \sum_i M_i = \mathbb{I}, M_i = M_i^\dagger \\ &\text{Variable} && M_i \end{aligned} \tag{3.27}$$

The optimization problem in Eq. (3.27) can be cast into a semidefinite program (SDP) using the procedure given in Appendix B. The SDP can be solved numerically using the `CVX` module [31], [30] on MATLAB to obtain the optimal POVM measurements.

3.4.2 Examples of Controller's Authority with Non-Maximal Svetlichny Inequality Violation

Though the CQT scheme works ideally where the tripartite state of Alice, Bob and Charlie is the GHZ state ($|\psi\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$), in reality the underlying state is a noisy GHZ state. Often errors are introduced while distributing the qubits which leads to decoherence. The final state ρ_f after a decoherence process ε is given by $\rho_f = \varepsilon\rho_i$. The action of ε can be described using Kraus operators $\{E_j\}_j$ in the following way [41]:

$$\varepsilon\rho_i = \sum_{j=1}^{M} E_j \rho_i E_j^\dagger \tag{3.28}$$

First, we will consider the case where the whole state is affected by the same decoherence process described by the total depolarizing channel. It is a process in which the ideal GHZ state is mixed with white noise with probability p. Thus,

$$\rho_f^{total} = p\frac{\mathbb{I}}{8} + (1-p)|\psi\rangle\langle\psi| \tag{3.29}$$

Next, we will consider the decoherence process in which each qubit of the tripartite GHZ state undergoes a depolarizing channel. Note that the qubit depolarizing process is physically more appropriate than the total depolarizing process because the three qubits are distributed to three different parties who are usually at different locations. Each qubit is coupled to its local environment and undergoes depolarizing independently though they were initially entangled at a single location. The qubit depolarizing channel is described

by the Kraus operators $E_0 = \sqrt{1-p'}I; \quad E_i = \sqrt{\frac{p'}{3}}\sigma_i$ where $p' = \frac{3p}{2}$. The final state after the qubit depolarizing process assuming the same depolarizing parameter for each quibit, is given by

$$\rho_f^{qubit} = \sum_{ijk} E_i \otimes E_j \otimes E_k \left|\psi\right\rangle \left\langle\psi\right| \left[E_i \otimes E_j \otimes E_k\right]^\dagger \tag{3.30}$$

$\rho_f^{total}, \rho_f^{qubit}$ are mixed states unless $p = 0$. One can think of these mixed states as a part of a bigger pure quantum state $\left|\psi^{ABCD}\right\rangle$ comprising Alice, Bob, Charlie and Derek such that $\mathrm{Tr}^D(\left|\psi^{ABCD}\right\rangle \left\langle\psi^{ABCD}\right|) = \rho_f^{qubit/total}$. In the language of quantum cryptography, one would say Derek 'holds' a purification of the mixed tripartite state. Since $\left|\psi^{ABCD}\right\rangle$ is a pure state, Derek is the most general eavesdropper. Any larger quantum system $\rho^{ABCD\Delta}$ with more eavesdroppers $\Delta_1, \Delta_2, \ldots, \Delta_N$ will be of the separable form $\rho^{ABCD\Delta} = \left|\psi^{ABCD}\right\rangle \left\langle\psi^{ABCD}\right| \otimes \rho^{\Delta_1,\Delta_2,\ldots,\Delta_N}$, which means that $\Delta_1, \Delta_2, \ldots, \Delta_N$ cannot be correlated with $\left|\psi^{ABCD}\right\rangle$.

In this thesis, we will use the spectral decomposition of a density matrix to obtain a purification of $\left|\psi^{ABCD}\right\rangle$ [60] from $\rho_f^{total/qubit}$. Any density matrix $\rho \in \mathrm{Herm}(\mathcal{H}_\mathcal{A})$, where $\mathcal{H}_\mathcal{A} \cong \mathbb{C}^\Sigma$ can be expressed as $\rho = \sum_{k\in\Sigma} \lambda_k \left|\Lambda_k\right\rangle \left\langle\Lambda_k\right|$. One way to purify ρ is to simply express $\left|\zeta\right\rangle = \sum_{k\in\Sigma} \sqrt{\lambda_k} \left|\Lambda_k\right\rangle \left|\Lambda_k\right\rangle$.

The purification $\left|\psi_f^{total/qubit}\right\rangle$ of $\rho_f^{total/qubit}$ is therefore given by

$$\left|\psi_f^{total/qubit}\right\rangle = \sum_{k\in\{1,2,\ldots,8\}} \frac{\rho_f^{total/qubit} \otimes \mathbb{I}_8 \left|\Lambda_k\right\rangle \left|\Lambda_k\right\rangle}{\sqrt{\mathrm{Tr} \left|\Lambda_k\right\rangle \left\langle\Lambda_k\right| \rho_f^{total/qubit}}} \tag{3.31}$$

Computing the Effective Control Power (ECP) for the Depolarized GHZ State

We have all the necessary ingredients to compute F_C^{NE} and F_{NC}^E (defined in Section 3.4) for the total depolarized and qubit depolarized GHZ states.

Let $\rho^B_{s_0 s_1 \gamma l}$ denote Bob's state when Alice and Charlie's boxes have revealed the outputs $s_0 s_1$ and γl after performing the measurements $\{M^{aA}_{s_0 s_1}\}_{s_0 s_1}$ and $\{M^C_{\gamma l}\}_{\gamma l}$ respectively.

$$\rho^B_{s_0 s_1 \gamma l} = \frac{\mathrm{Tr}^{aAC}(\frac{\mathbb{I}+\vec{a}.\vec{\sigma}}{2} \otimes \rho_f^{total/qubit} M^{aA}_{s_0 s_1} \otimes \mathbb{I} \otimes M^C_{\gamma l})}{\mathrm{Tr}\left(\frac{\mathbb{I}+\vec{a}.\vec{\sigma}}{2} \otimes \rho_f^{total/qubit} M^{aA}_{s_0 s_1} \otimes \mathbb{I} \otimes M^C_{\gamma l}\right)}$$

Then the average fidelity of teleportation with Charlie's permission is given by:

$$F_C^{NE} = \int \frac{d\vec{a}}{4\pi} \sum_{s_0,s_1,l \in \{0,1\};\ \gamma \in \{\pm 1\}} P(s_0 s_1 \gamma l) \langle a| R^{-1}_{s_0 s_1 \gamma l} \rho^B_{s_0 s_1 \gamma l} (R^{-1}_{s_0 s_1 \gamma l})^\dagger |a\rangle \tag{3.32}$$

Remark 2. *Fixed rotation matrices $R^{-1}_{s_0 s_1 \gamma l}$: The calculation of F_C^{NE} has been done assuming that the corrective rotations ($R^{-1}_{s_0 s_1 \gamma l}$) of Bob are those that are required to exactly recover the qubit to be teleported, had the shared tripartite state ($\rho_f^{total/qubit}$) been the perfect GHZ state. In this chapter, the rotation matrices $R^{-1}_{s_0 s_1 \gamma l}$ have been assumed to be fixed. We have not considered variable rotations conditioned on the underlying tripartite state.*

To compute F^E_{NC}, we first need to determine the optimal POVMs of Derek which will execute the adversarial strategy (Section 3.4.1).

ρ^{ABD} can be obtained from $\rho_f^{total/qubit}$ by first purifying it into $\left|\psi_f^{total/qubit}\right\rangle$ [Eq. (3.31)] and then tracing out Charlie's system.

$$\rho^{ABD} = \mathrm{Tr}^C(\left|\psi_f^{total/qubit}\right\rangle \left\langle\psi_f^{total/qubit}\right|) \tag{3.33}$$

By substituting ρ^{ABD} in the expression $\tilde{\rho}_i = \mathrm{Tr}^D(|\phi_i\rangle \langle\phi_i| \otimes \mathbb{I}\rho^{ABD})$, one can set up the optimization given in Eq. (3.27).

Derek can then use the optimal POVMs $\{M_i\}_i$ to measure his system and reveal $\delta = i \in \{(+1)0, (+1)1, (-1)0, (-1)1\}$ to Bob. Hence, Alice and Bob's joint state (ρ_i^{AB}) conditioned on the result of Derek's measurement is given by:

$$\rho_i^{AB} = \frac{\mathrm{Tr}^D(\rho^{ABD} \otimes \mathbb{I}_2 \otimes \mathbb{I}_2 \otimes M_i)}{\mathrm{Tr}(\rho^{ABD} \otimes \mathbb{I}_2 \otimes \mathbb{I}_2 \otimes M_i)} \tag{3.34}$$

Now Alice performs the Bell measurement $\{M^{aA}_{s_0 s_1}\}_{s_0 s_1}$ on the state to be teleported and her share of the composite state ρ_i^{AB}. After Alice reveals her measurement outcome, Bob's qubit is prepared in the following state:

$$\rho^B_{s_0 s_1 i} = \frac{\mathrm{Tr}^{aA}(\frac{\mathbb{I}+\vec{a}.\vec{\sigma}}{2} \otimes \rho_i^{AB} M^{aA}_{s_0 s_1} \otimes \mathbb{I})}{\mathrm{Tr}\left(\frac{\mathbb{I}+\vec{a}.\vec{\sigma}}{2} \otimes \rho_i^{AB} M^{aA}_{s_0 s_1} \otimes \mathbb{I}\right)} \tag{3.35}$$

Finally, the average fidelity of teleportation without Charlie's permission but with Derek's assistance (F^E_{NC}) can be computed.

$$F^E_{NC} = \int \frac{d\vec{a}}{4\pi} \sum_{s_0,s_1 \in \{0,1\};\ i \in \{0,1\}^2} P(s_0 s_1 i) \langle a| R^{-1}_{s_0 s_1 i} \rho^B_{s_0 s_1 i} (R^{-1}_{s_0 s_1 i})^\dagger |a\rangle \tag{3.36}$$

Svetlichny Inequality Violation for Depolarized GHZ States

We use the physical interpretation of the total depolarized GHZ state (TDGHZ) and the qubit depolarized GHZ state (QDGHZ) to derive the maximum Svetlichny inequality violation that can be obtained for a given depolarizing channel parameter.

As mentioned earlier, the total depolarized GHZ state can be seen as a probabilistic mixture of the perfect GHZ state ($\frac{|000\rangle+|111\rangle}{\sqrt{2}}$) and the completely mixed three qubit state ($\frac{\mathbb{I}}{8}$).

The qubit depolarizing channel can be described by the process in which each qubit can get replaced by the completely mixed single qubit state ($\frac{\mathbb{I}}{2}$), with probability p. For the GHZ state, it means that with probability $(1-p)^3$ the state is unaltered; with probability $3p(1-p)^2$, the GHZ state is transformed into a bipartite entangled state and with probability $3p^2(1-p)+p^3$, it is transformed into a separable state.

It was shown in Ref. [72] that tripartite entangled states are required for violating the Svetlichny Inequality ($S \leq 4$). Bipartite entangled states and separable states do not violate this inequality while the tripartite entangled perfect GHZ state ($\frac{|000\rangle+|111\rangle}{\sqrt{2}}$) violates it maximally ($S = 4\sqrt{2}$). Moreover, according to Claim 1 it is possible to achieve the ($S \leq 4$) bound using classical strategies. Therefore, the maximum Svetlichny inequality violation is given by the following equations:

$$S_{TDGHZ} = (1-p)S_{GHZ} + pS_{Classical} \tag{3.37}$$
$$= (1-p)4\sqrt{2} + 4p \tag{3.38}$$
$$S_{QDGHZ} = (1-p)^3 S_{GHZ} + (1-(1-p)^3)S_{Classical} \tag{3.39}$$
$$= (1-p)^3 4\sqrt{2} + 4(1-(1-p)^3) \tag{3.40}$$

3.4.3 Numerical Results Demonstrating the Trend Between Effective Control Power and Svetlichny Violation

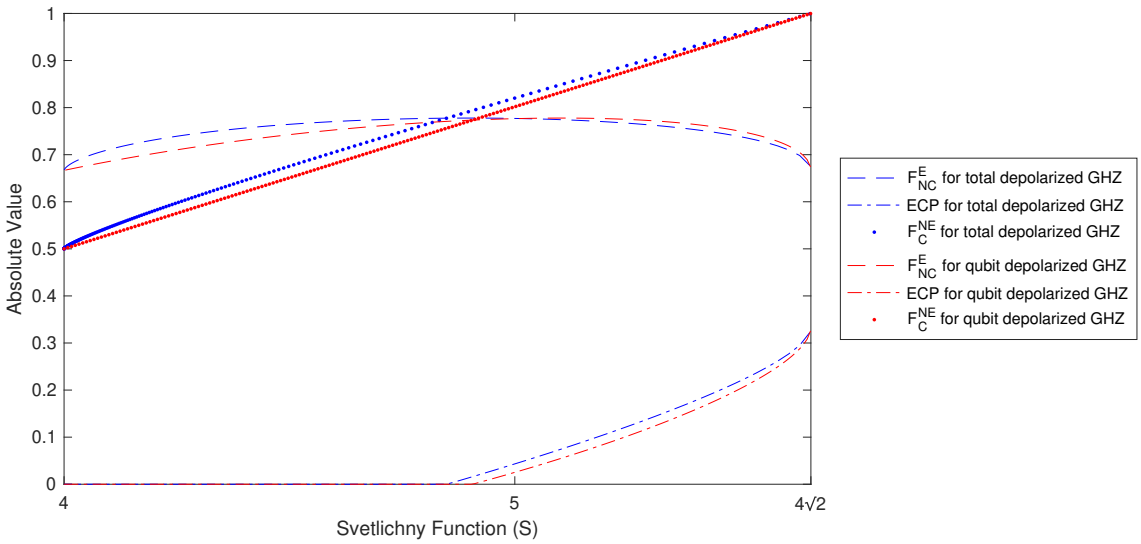


Figure 3.4: Effective Control Power (ECP), average fidelity of teleportation with controller's permission (F_C^{NE}) and average fidelity of teleportation without controller's permission but with eavesdropper's participation (F_{NC}^{E}) as a function of maximum Svetlichny inequality violation (S) given by Eq. (3.37) for both the qubit depolarized and total depolarized GHZ states with parameter $p \in (0, 1)$

For a given depolarizing parameter $p \in (0, 1)$, the maximum Svetlichny inequality violation was computed using Eq. (3.37). The Effective Control Power (ECP) was computed using the method described in Section 3.4.2 and plotted against the maximum Svetlichny violation corresponding to the given value of parameter p. It is interesting to note that ECP is positive only when $S > 4.84$ for the total depolarized GHZ state and when $S > 4.90$ for the qubit depolarized GHZ. The plots clearly show that ECP is a monotonically increasing function of S. The highest value of ECP is reached at the maximal violation of Svetlichny's inequality which confirms our Claim 2. It is important to note that the violation of the Svetlichny inequality [Eq. (3.21)] does not necessarily imply that Charlie has positive control power. For non-maximal violation, there is a small window in the range $4.84 < S < 4\sqrt{2}$ for the qubit depolarized GHZ states and $4.90 < S < 4\sqrt{2}$ for the total depolarized GHZ states, where ECP is positive.

3.5 Summary and Outlook

In this chapter, we have performed a device independent study of controlled teleportation of a qubit with an untrusted receiver. We constructed a device independently testable scenario in a way that allowed us to certify in the context of controlled teleportation, whether quantum resources were being used by the device despite the receiver being untrusted. We found in this case that the well-known Svetlichny inequality must be violated to certify quantum correlations. A maximal violation of the Svetlichny inequality guarantees maximum control power. This is in contrast to the controlled teleportation with all trusted parties where the maximal violation of Mermin's inequality was sufficient to certify maximum control power. This indicates that a stronger form of nonlocality, also known as 'genuine tripartite nonlocality', is required to device independently test the controlled quantum teleportation with an untrusted receiver.

We proposed an adversarial strategy, not proven to be optimal, which can effectively decrease the controller's authority by taking advantage of a non-ideal device that non-maximally violates the Svetlichny inequality. By taking the example of two families of quantum states characterized by the total depolarized and the qubit depolarized GHZ states, we showed that controller's authority is a monotonically increasing function of the maximal Svetlichny inequality violation. For the given family of depolarized GHZ states, adversarial strategy and a Svetlichny inequality violation, one can infer the controller's authority from our numerically obtained plot. We found a window of non-maximal Svetlichny inequality violation where the controller's authority is non-zero. This shows that the controlled teleportation scheme with an untrusted receiver is robust to depolarizing noise present in the device.

A natural next step would be to investigate whether the eavesdropping strategy considered in Section 3.4.2 is optimal. It would be useful to find out whether there exists any better eavesdropping strategy for the depolarized GHZ state that would reduce the effective control power even further.

A practical way to extend this work would be to consider both the sender (Alice) and the receiver (Bob) to be untrusted parties. In that case, the criteria for device -independent certification will change. Svetlichny's Inequality violation may no longer be sufficient to confirm that the underlying source of correlations is quantum.

Chapter 4

Implementation of Quantum Lightning

4.1 Introduction

Quantum Money is a theoretical method of payment in which the role of bank notes is played by quantum states. A quantum money scheme typically consists of a bank note (which is a quantum state associated with a unique serial number) generating process and a verification procedure of the bank notes. It is appealing because of two reasons: *(i)* quantum no-cloning theorem implies that the bank notes generated by this process cannot be copied. *(ii)* Fast transfer of bank notes can be done using quantum teleportation. In the first quantum money scheme introduced by Weisner, the generation and verification processes were both done by the bank. The major limitation of this scheme is that it is required to send a note back to the mint for verification using a a secret classical description held by the mint. In a Public Key Quantum Money (PKQM) [2] scheme, the verification process is made public i.e., anyone with a bank note can verify it. Despite that, it is impossible for anyone except the mint to generate new bank notes. Recently, **Quantum Lightning** (https://arxiv.org/abs/1711.02276) was introduced, which is a strengthening of the PKQM scheme. In Quantum Lightning, the generating procedure is also made public along with the verfication procedure. Despite that, no computationally bounded adversary can deviate from the generating procedure called 'storm' in such a way that it can produce two bank notes also called 'bolts' with the same serial number, both of which pass the verification procedure. The security notion of this scheme relies on the hardness assumption of a classical computational problem. It has possible applications not only in

quantum money but also in random number generation and cryptocurrency.

The interesting nomenclature of this scheme is rooted in the way bolts are generated. A generating procedure should be such that a unique bolt is produced every time or the same bolt is never produced twice, just like the claim of the old adage: "lightning never strikes the same place twice". Since a classical procedure can in principle be deterministically reproduced given the correct initial conditions, it is not sufficient to use a classical procedure for generating unique bolts. The generating procedure has to rely on the quantum property of no-cloning. Hence, the name 'quantum lightning'.

Zhandry proposed a quantum lightning construction in [85]. In this chapter, we examine the implementation of this construction in the form of quantum circuits on qubits. In Section 4.2, we present the quantum lightning scheme in more detail. In Section 4.3, we review Zhandry's construction of quantum lightning. We present our quantum circuit implementation of an important part of the construction and lay out the difficulties of implementing others in Section 4.4. We summarize and discuss future directions in Section 4.5.

4.2 Quantum Lightning Scheme

The quantum lightning scheme is based on the non-affine multi-collision resistance of degree-2 polynomial hash functions. These hash functions are specified by n polynomials $P_1, P_2, \ldots, P_n$ in m variables. If $m \approx rn$, it has been conjectured that it is impossible to devise 2(r+1) colliding inputs that have no affine relations.

Based on the above conjecture, the quantum lightning scheme was constructed. A bolt can be generated by taking $r+1$ copies of the superposition of the pre-images of the hash function $f_{\mathcal{A}}$ corresponding to a particular output. To generate a superposition, $f_{\mathcal{A}}$ is applied on a uniform superposition created over the domain of $f_{\mathcal{A}}$ and the output is stored on a second register. When the second register is measured, one obtains y as the serial number and the first register is prepared in a uniform superposition of the pre-images of y. The first register is the superposition state and the second register is the serial number. A bolt comprises $r+1$ copies of these superposition states all of which correspond to the same serial number. Suppose it were possible to generate two bolts with the same serial number y. On measurement of the bolts in computational basis, it is very likely that one would obtain different pre-images for each copy of the superposed pre-image state - a total of $2(r+1)$ pre-images corresponding to a single image. This would violate the conjecture that it is impossible to find $2(r+1)$ colliding inputs of $f_{\mathcal{A}}$. The quantum lightning scheme

can be seen as an analog of collision resistance where an adversary tries to device two inputs which hash to the same value. In quantum lightning, an adversary tries to devise two bolts which hash to the same serial number.

There are three steps in this construction. The first step is called `Setup` in which the public verification key is sampled. `Gen` is the bolt generation step, and `Ver` is the bolt verification step. Each of these steps will be described in detail. Before that, we will discuss the computational hardness assumption that is crucial to this construction.

4.2.1 Background and Hardness Assumptions

Consider a sequence of upper triangular matrices $\mathcal{A} = (A_1, A_2, ..., A_n)$ with elements in $\mathbb{F}_2$. Then, degree-2 polynomial functions in x can be expressed in general as follows:

$$f_{\mathcal{A}}(x) : \{0,1\}^m \longrightarrow \{0,1\}^n$$

$$f_{\mathcal{A}}(x) = (x^T A_i x)_i$$

Since $x^2 = x$, the linear terms come from the diagonal and the cross terms give the quadratic terms.

Suppose we want to find collisions for $f_{\mathcal{A}}$ i.e., two inputs for which $f_{\mathcal{A}}$ gives the same output. Choose a Δ randomly from the set $\{0,1\}^m$. The condition for collision precisely means:

$$x^T A_i x = (x - \Delta)^T A_i (x - \Delta)$$

Or,

$$\Delta^T A_i \Delta = \Delta^T (A_i + A_i^T) x$$

This forms a set of n equations in m unknowns.

Now consider a matrix B whose rows are $\Delta^T(A_i + A_i^T)$. As long as B has rank n (full rank), a solution for x is guaranteed (given $n < m$). Since Δ is chosen randomly and A_i are random upper triangular matrices, B can be row reduced with a constant probability (constant w.r.t. choice of A_i's and Δ.)

Now, suppose we want to find $(k+1)$ collisions instead of 2 in a k dimensional affine space such that those $k+1$ points do not lie in a $k-1$ dimensional affine space. In other words, we don't want those $k+1$ points to have affine relations (non-affine, analogous to non linear). Choose randomly $\Delta_1, \Delta_2, ..., \Delta_n$. This time, The B matrix will be less fat as

$B = B_{\Delta_1,\Delta_2,...,\Delta_k}$. B will be a $nk \times m$ matrix. As long as $nk \leq m$ and B has full rank, a solution is guaranteed. Again, B will be full rank with constant probability since $\Delta's$ and $A_i's$ are chosen randomly and with overwhelming probability if $nk + \omega log(\lambda) \leq m$. Here λ is the security parameter and it can be chosen according to specific requirements.

Definition 1. *A function f is called (k+1)-Non Affine Multi Collision Resistant (NAMCR) if it is computationally hard to find (k+1) colliding inputs such that f gives the same output for all of them.*

Assumption 1. *Let $k = poly(n)$ and $m < (k + 1/2)n$. Choose random upper triangular matrices $A_i \in \{0,1\}^{m \times m}$ and set $\mathcal{A} = (A_1, A_2, ..., A_n)$. Then $f_{\mathcal{A}}$ is $2(k + 1)$ NAMCR. i.e.,*

$$Pr[\{x_1, x_2, ..., x_{2(k+2)}\} \text{ all of which collide in } f_{\mathcal{A}}] \text{ is negligible}$$

4.2.2 General Properties of a Quantum Lightning Scheme

The main component in a QL scheme is the 'bolt' which is a quantum state denoted by $|\lightning\rangle$. A Generating algorithm called `Gen` is a quantum polynomial time algorithm that takes as input a security parameter λ and generates a new bolt ($|\lightning\rangle$). `Ver` is a quantum polynomial time algorithm that verifies a valid bolt and extracts its serial number; otherwise it outputs $\perp$.

The requirements for **correctness** of a Quantum Lightning scheme are as follows:

- `Ver` always accepts $|\lightning\rangle$ generated by `Gen`.
- `Ver` does not perturb the $|\lightning\rangle$
- `Ver` outputs the same serial number for a given bolt every time. In other words, the serial number is a deterministic function of $|\lightning\rangle$.

The **security** notion of a Quantum Lightning scheme can be seen as the following experiment between challenger and adversary:

- The challenger generates a `(Gen,Ver)` pair depending on security parameter λ and sends `(Gen,Ver)` to adversary who possesses a malicious bolt generating storm `GenMal`.
- `GenMal` produces two potentially entangled bolts $|\lightning_0\rangle$, $|\lightning_1\rangle$ and sends them to the challenger.

- The challenger runs `Ver` on $|\lightning_0\rangle$, $|\lightning_1\rangle$ and produces two serial numbers s_0 and s_1. The challenger accepts only if $s_0 = s_1 \neq \perp$, i.e., the challenger accepts defeat by the adversary.

A valid construction of Quantum Lightning scheme must satisfy the above security requirements. A quantum lightning scheme can be converted into a quantum money scheme by combining it with digital signatures [86, 2]. A valid bank note would be a bolt state with an associated serial number and its digital signature. This prohibits an adversary from generating new bank notes with new serial numbers. It is therefore required that the adversary must break the quantum lightning scheme to break the corresponding quantum money scheme, i.e., it must generate two valid bolt states, both of which are accepted by the `Ver` algorithm.

4.3 Zhandry's Construction of Quantum Lightning

Using the above assumption and mathematical setting, the following scheme was constructed by the author for Quantum Lightning.

- `Setup`: Choose n random upper-triangular matrices $\mathbf{A} \in \{0,1\}^{m\times m}$ and define $\mathcal{A} = \{\mathbf{A}_i\}_i$. Make $\mathcal{A}$ public.
- Bolt generation (`Gen`): Make a superposition of $(k+1)$ colliding inputs. The result is statistically close to $(\sum_{x:f_{\mathcal{A}}(x)=z}|x\rangle)^{\otimes(k+1)} \propto |\lightning'_z\rangle^{\otimes(k+1)}$.
- Verification (`Ver`): To verify a bolt, one needs to run a verification on each of the (k+1) mini-bolts. If all of them give the same value y, only then it is accepted otherwise it is rejected. Thus the algorithm outputs in the set $\{0,1\}^n \cup \perp$. This process involves two steps. Now the mini-verifications proceed as follows. First it must be ensured that each mini-bolt to be verified ($|\phi\rangle$) belongs to the span of $\{|\lightning'_z\rangle\}_z$. If $|\phi\rangle$ fails this test then output $\perp$ immediately. Otherwise proceed to the second step where the function $f_{\mathcal{A}}$ is evaluated in superposition to obtain y without changing the original state of $\{|\lightning'\rangle\}$. If the end result is $(y, y, ..., y)$, a list of (k+1) elements, then output y. Otherwise output $\perp$. Clearly, any invalid bolt will be rejected because by definition they will not yield the same serial number for all mini-bolts. Also, each valid bolt will be accepted with certainty. Thus, this scheme is correct (Section 4.2.2). The mathematical details of these two steps involves multiple linear algebra tricks as described in Zhandry's paper [85].

4.3.1 Security

Adversarial Goal: The adversary is a malicious bolt generation procedure (`GenMal`) that tries to produce two bolts $\{|\lightning_0\rangle\}$ and $\{|\lightning_1\rangle\}$ such that both of them are accepted by `Ver` and have the same serial number.
Adversarial Capabilities: The adversarial bolt generating procedure `GenMal`, has to be computationally efficient in the number of qubits comprising each mini-bolt (n).

Theorem 1. *If Assumption 1 holds true then the quantum lightning scheme (Section 4.3) is secure.*

Proof. Let the adversary produce with non-negligible probability, two bolts $|\lightning_0\rangle$ and $|\lightning_0\rangle$ using `GenMal`, both of which pass the verification procedure `Ver` such that `Ver` extracts the same serial number $s_0 = s_1 = s$ from both.

According to the scheme (Section 4.3), this means that the composite state of the two bolt states is $|\lightning_0\rangle \otimes |\lightning_1\rangle = \{|\lightning'_s\rangle\}^{\otimes(k+1)} \otimes \{|\lightning'_s\rangle\}^{\otimes(k+1)} = \{|\lightning'_s\rangle\}^{\otimes 2(k+1)}$.

On measuring each mini-bolt of the composite state $\{|\lightning'_s\rangle\}^{\otimes 2(k+1)}$ one obtains $2(k+1)$ random inputs to the function $f_{\mathcal{A}}$, all of which correspond to the same output s.

But, the Assumption 1 states that it is computationally infeasible to find $2(k+1)$ colliding inputs to the function $f_{\mathcal{A}}$. Since `GenMal` is restricted to be computationally efficient, it leads to a contradiction.

It follows that if Assumption 1 holds true then `GenMal` cannot produce two valid bolts with the same serial number. Hence, the quantum lightning scheme is secure under Assumption 1. □

4.4 Circuit Implementation of Quantum Lightning

An important operation for both the `Gen` and the `Ver` steps (Section 4.3) is to evaluate the function $f_{\mathcal{A}}(x) = (x^T A_i x)_i$. In this section, we will present the circuit construction of the evaluation of the function. Let $A \in \{0,1\}^{m\times m}$ and $x \in \{0,1\}^m$. Using the following command on matlab n times, one can generate n upper triangular matrices $A_i \in \{A_1, A_2, ..., A_n\}$ in a pseudorandom manner: `A=triu(randi([0,1],m))`. $x^T Ax$ is given by the following circuit model:

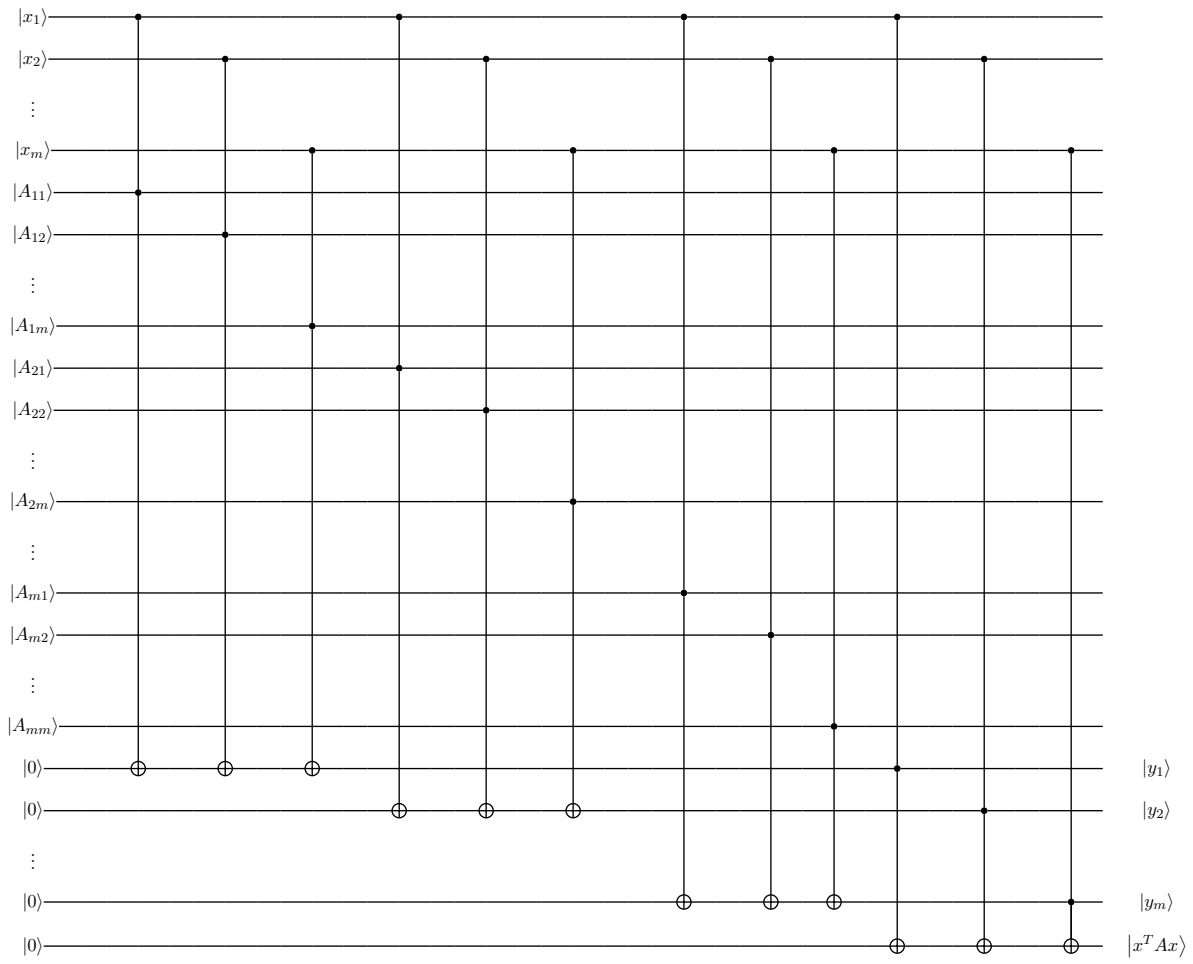


Figure 4.1: Circuit model of $x^T Ax$. Here $x_1 x_2 \dots x_m = x$. $A = \{A_{ij}\}_{i,j}$

This is represented by the following contracted circuit:

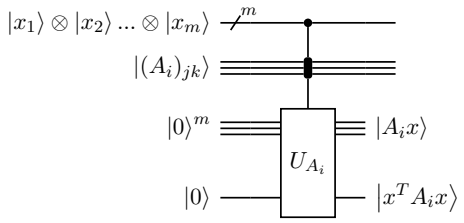


Figure 4.2: Abstract circuit model of $x^T A_i x$

Combining the above circuits, we get the final circuit model of $f_{\mathcal{A}}(x) = (x^T A_1 x, x^T A_2 x, ..., x^T A_n x)$.

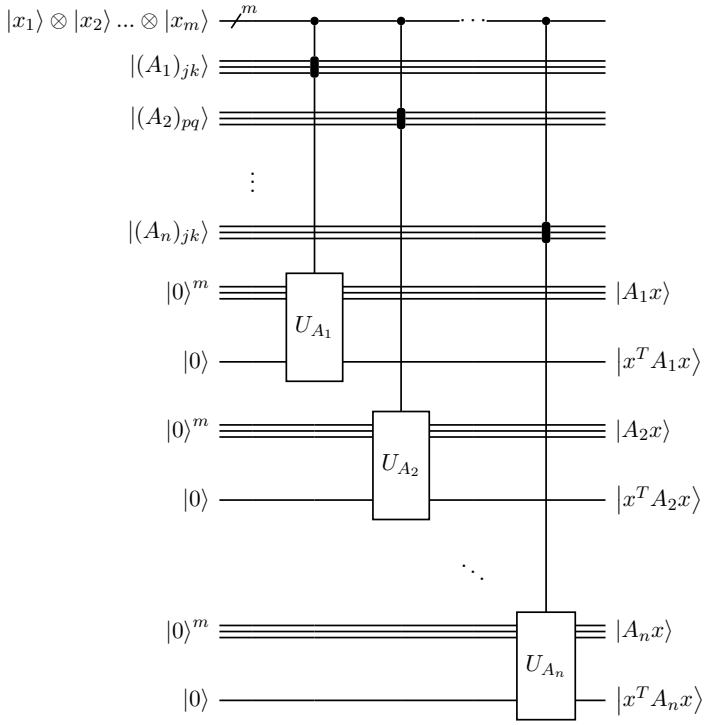


Figure 4.3: Circuit model of $f_{\mathcal{A}}(x) = (x^T A_1 x, x^T A_2 x, ..., x^T A_n x)$.

4.4.1 Verification

Recap: A valid bolt is given by $(\sum_{x:f_{\mathcal{A}}(x)=z} |x\rangle)^{\otimes(k+1)} \propto \left|\mathcal{F}'_z\right\rangle^{\otimes(k+1)}$. Each $\left|\mathcal{F}'_z\right\rangle$ is called a minibolt. All the $k+1$ minibolts together constitute the quantum lightning bolt. The verification algorithm must run on each minibolt individually. The verification problem can be expressed as the following statement:

Verification Problem: Find an efficient algorithm (involving a number of evaluations that scales polynomially in m and n) that checks whether an arbitrary m qubit state, $|\phi\rangle$, is a valid minibolt such that at the end of the algorithm, a valid minibolt state is unaltered.

$$\texttt{if } |\phi\rangle \in \{\left|\mathcal{F}'_y\right\rangle\}_y \text{ as y varies}$$

$$\texttt{then output}(1, |\phi\rangle)$$

$$\texttt{else output}(0, |\phi'\rangle)$$

where $|\phi'\rangle$ may not be the same as $|\phi\rangle$.

Zhandry's solution sketch:

1. Prove that $\left|\mathcal{F}'_y\right\rangle$ and $|\phi_r\rangle = \sum_r (-1)^{r.f_{\mathcal{A}}(x)} |x\rangle$ span the same linear space.

2. Express

$$\left|\mathcal{F}'_y\right\rangle = \sum_r \alpha_r |\phi_r\rangle, \quad r \in \{0,1\}^n \tag{4.1}$$

$$= \sum_{r,x} \alpha_r (-1)^{r.f_{\mathcal{A}}(x)} |x\rangle \tag{4.2}$$

   Thus, it is sufficient to check whether

$$|\phi\rangle \in \sum_r \alpha_r |\phi_r\rangle$$

3. Perform the following algorithm steps:

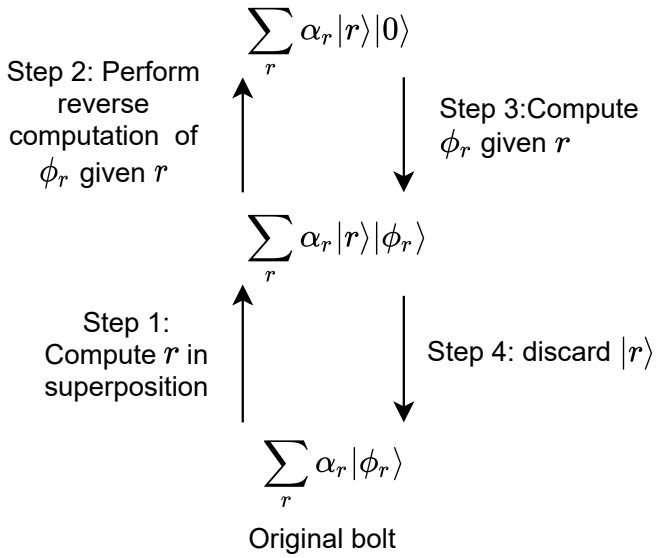


Figure 4.4: Verification Algorithm

If $|\phi\rangle \notin \sum_r \alpha_r |\phi_r\rangle$, the last qubit of the state obtained after step 2 will not be $|0\rangle$. The verification procedure accepts a bolt only if the measurement outcome in computational basis of the last register after Step 2 is 0.
Step 3 of the algorithm is easily performed by applying a Hadamard gate on $|0\rangle$, followed by controlled phase gate $(-1)^{r.f_A(x)}$.

Step 2 is the reverse computation of Step 3.

Step 4 is the trivial step where qubits containing $|r\rangle$ are discarded.

The only remaining step is step 1. The author claims that it is sufficient to estimate r, given $|\alpha_r\rangle$. The method for estimation in the paper involves measurements in the computational basis on multiple qubits of $|\alpha_r\rangle$. Since the bolt state will be in a superposition of the form $|\phi\rangle \in \sum_r \alpha_r |\phi_r\rangle$, performing a measurement will collapse the state, which can irreversibly alter the bolt state. It is not clear whether there is a way to estimate r from $|\alpha_r\rangle$ in a non-destructive way. Thus, the following problem remains to be solved in order to complete the verification algorithm:

$$\text{transform } \sum_r \alpha_r |\phi_r\rangle \longrightarrow \sum_r \alpha_r |r\rangle |\phi_r\rangle \tag{4.3}$$

Alternatively, one could use an entirely different approach for verification and that would take us back to the original problem 4.4.1.

4.5 Summary and Outlook

In this chapter, we introduced the ideas of quantum money and its strengthening, namely, quantum lightning. We reviewed the requirements of a valid quantum lightning scheme, and also discussed a specific construction. We presented quantum circuits implementing the degree 2 polynomial function that plays an important role in the scheme. Finally, we clearly identified the step in its verification algorithm of which an implementation is unclear.

Although the idea of quantum lightning is fascinating, a readily implementable quantum lightning scheme does not exist. A future direction is to find an implementation of the verification problem as stated in Section 4.4.1. One could attempt to use a suitable modification of the Grover's search algorithm for this purpose. Another future direction is to investigate whether the quantum circuit implementing the degree-2 polynomial function can be optimized further to reduce the number of gates. The hardness assumption was broken in a slightly different version of the construction than that presented in this thesis [69]. It remains an open question to device a similar attack on this version, eventually breaking the security proof. One can also attempt to suitably modify the verification algorithm such that this hardness assumption can still be used to construct quantum lightning.

Chapter 5

Summary

In Chapter 2, we studied the quantum simulation of the quantum kicked top (QKT) - a periodically driven spin system that undergoes chaotic dynamics in the classical limit. Our results demonstrate the advantages of circuit-based NISQ devices for exploring fundamental questions in quantum information and quantum chaos despite their noise and scale limitations.

We reviewed the QKT model which can be described as a collection of a fixed number of spin-1/2 particles. We highlighted the importance of entanglement in the study of quantum-classical correspondence using the QKT. After a short review of laboratory experiments implementing the QKT, we have proposed a quantum circuit-based approach to simulate and explore quantum chaos and demonstrated its advantages over existing methods. The proposed method can be applied in general to any periodically driven finite-dimensional quantum system.

In our study, IBM's 5-qubit open access quantum chip (Vigo) was used as the experimental platform to implement the proposed approach for the 2-qubit quantum kicked top (QKT). The Hamiltonian of the QKT can be exactly expressed in terms of qubits since it is a finite-dimensional quantum system. Therefore, its evolution operator can be decomposed into quantum gates. Traditionally, experimental studies of quantum chaos have applied the same set of operations n times to explore time evolution. Here, we decomposed the unitary evolution operator for n kicks, U^n, into elementary quantum gates. This results in a fixed number of operations implementing the QKT evolution for any number of kicks. This hybrid combination of classical processing and quantum computing opens up the ability to perform high fidelity experimental studies of quantum chaos in new parameter regimes. Since the value of the chaoticity parameter κ only determines the parameters of

unitary rotations in the quantum circuit, and since the single qubit rotation errors are independent of the parameters, we were able to experimentally study chaotic dynamics over a wider range of κ and kick number compared to previous studies. By taking advantage of the high fidelity obtained for both a large number of kicks and arbitrary κ values, we experimentally demonstrated the periodicity of entanglement with time and κ with high accuracy. Our studies also clearly showed signatures of chaos in the contour plot of average 2-qubit concurrence despite being in the deeply quantum regime. We also reported the first observation of the correspondence between average entanglement and delocalization in the 2-qubit QKT.

There are a number of avenues for further exploration of this topic. By applying error correction to the proposed circuit approach, our results could be improved even further. The scheme used in this paper for the decomposition of an arbitrary unitary into elementary quantum gate requires exponentially many classical operations for higher values of j. This could make the realization of QKT consisting of several qubits computationally expensive. However, physical effects such as bifurcation are more pronounced in the QKT for higher j(~ 100 qubits) [11]. To effectively observe bifurcation, it is necessary to use an efficient decomposition scheme. The symmetries in the floquet operator of the QKT could allow a more efficient decomposition scheme. We have suggested a promising approach that uses the Quantum Schur Transform.

In Chapter 3, we studied the controlled quantum teleportation of a qubit in the presence of an adversary. First, we reviewed the standard teleportation protocol and then described the formalism of controlled teleportation protocol involving three parties. We discussed the role of nonlocality in the certification of quantum resources used for the standard teleportation protocol. We constructed a device independently testable scenario in a way that allowed us to certify in the context of controlled teleportation, whether quantum resources were being used by the device despite the receiver being untrusted. We found in this case that the well-known Svetlichny inequality must be violated to certify quantum correlations. A maximal violation of the Svetlichny inequality guarantees maximum control power. This is in contrast to the controlled teleportation with all trusted parties where the maximal violation of Mermin's inequality was sufficient to certify maximum control power. This indicates that a stronger form of nonlocality is required to device independently test the controlled quantum teleportation with an untrusted receiver.

We proposed an adversarial strategy, not proven to be optimal, which can effectively decrease the controller's authority in a non-ideal device that non-maximally violates the Svetlichny inequality. By taking the example of the total depolarized and the qubit depolarized GHZ states, we showed that the controller's authority is a monotonically increasing function of the maximal Svetlichny inequality violation. For the given family of depolar-

ized GHZ states, adversarial strategy and a Svetlichny inequality violation, we numerically quantified the controller's authority. We found a window of non-maximal Svetlichny inequality violation where the controller's authority is non-zero. This shows that the controlled teleportation scheme with an untrusted receiver is robust to depolarizing noise present in the device.

Multiple extensions to this work are possible. An interesting avenue would be to investigate whether the eavesdropping strategy considered in Section 3.4.2 is optimal. It would be useful to find out whether there exists any better eavesdropping strategy for the depolarized GHZ state that would reduce the effective control power even further. A practical way to extend this work would be to consider both the sender (Alice) and the receiver (Bob) to be untrusted parties. In that case, it would be necessary to explore whether Svetlichny inequality violation is sufficient to confirm that the underlying source of correlations is quantum.

In Chapter 4, we studied the quantum circuit implementation of a cryptographic object called quantum lightning. We reviewed the concept of quantum money and discussed its strengthening, namely, quantum lightning. We described an existing construction of quantum lightning that relies on degree-2 polynomial functions. We built the quantum circuit implementing degree-2 polynomials that involves extensive entangling operations. We identified a step in the verification algorithm of which the implementation in terms of quantum circuits is unclear. Finally, we noted that the computational hardness assumption used in this construction was broken in a slightly different version. This could lead to a possible attack on this construction of quantum lightning.

References

[1] Qiskit 0.23.2 documentation — qiskit 0.23.2 documentation.

[2] Scott Aaronson, Jiahui Liu, and Ruizhe Zhang. Quantum copy-protection from hidden subspaces. *arXiv preprint arXiv:2004.09674*, 2020.

[3] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97:120405, Sep 2006.

[4] Dave Bacon, Isaac L Chuang, and Aram W Harrow. The quantum schur and clebsch-gordan transforms: I. efficient qudit circuits. In *Proceedings of the eighteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 1235–1244, 2007.

[5] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio. Definitions of multipartite nonlocality. *Phys. Rev. A*, 88:014102, Jul 2013.

[6] Jean-Daniel Bancal, Cyril Branciard, Nicolas Gisin, and Stefano Pironio. Quantifying multipartite nonlocality. *Phys. Rev. Lett.*, 103:090503, Aug 2009.

[7] Artur Barasiński, Antonín Černoch, and Karel Lemr. Demonstration of controlled quantum teleportation for discrete variables on linear optical devices. *Phys. Rev. Lett.*, 122:170501, Apr 2019.

[8] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[9] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[10] S. Bettelli and D. L. Shepelyansky. Entanglement versus relaxation and decoherence in a quantum algorithm for quantum chaos. *Phys. Rev. A*, 67:054303, May 2003.

[11] Udaysinh T. Bhosale and M. S. Santhanam. Periodicity of quantum correlations in the quantum kicked top. *Phys. Rev. E*, 98:052228, Nov 2018.

[12] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[13] Davide Castelvecchi. The quantum internet has arrived (and it hasn't). *Nature*, 554(7692), 2018.

[14] Daniel Cavalcanti, Antonio Acín, Nicolas Brunner, and Tamás Vértesi. All quantum states useful for teleportation are nonlocal resources. *Phys. Rev. A*, 87:042104, Apr 2013.

[15] S Chaudhury, A Smith, BE Anderson, S Ghose, and Poul S Jessen. Quantum signatures of chaos in a kicked top. *Nature*, 461(7265):768–771, 2009.

[16] Rafael Chaves, Daniel Cavalcanti, and Leandro Aolita. Causal hierarchy of multipartite Bell nonlocality. *Quantum*, 1:23, August 2017.

[17] Shruti Dogra, Vaibhav Madhok, and Arul Lakshminarayan. Quantum signatures of chaos, thermalization, and tunneling in the exactly solvable few-body kicked top. *Phys. Rev. E*, 99:062217, Jun 2019.

[18] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[19] H. Fan, K. Matsumoto, and H. Imai. Quantify entanglement by concurrence hierarchy. *Journal of Physics A: Mathematical and General*, 36:4151–4158, 03 2003.

[20] AT Fuller. Lyapunov centenary issue. *International Journal of Control*, 55(3):521–527, 1992.

[21] Guillermo García-Pérez, Matteo AC Rossi, and Sabrina Maniscalco. Ibm q experience as a versatile experimental testbed for simulating open quantum systems. *npj Quantum Information*, 6(1):1–10, 2020.

[22] Guillermo García-Pérez, Matteo AC Rossi, and Sabrina Maniscalco. Ibm q experience as a versatile experimental testbed for simulating open quantum systems. *npj Quantum Information*, 6(1):1–10, 2020.

[23] George, Ian. Numerical finite key analysis. Master's thesis, 2020.

[24] B. Georgeot and D. L. Shepelyansky. Emergence of quantum chaos in the quantum computer core and how to manage it. *Phys. Rev. E*, 62:6366–6375, Nov 2000.

[25] B. Georgeot and D. L. Shepelyansky. Quantum chaos border for quantum computing. *Phys. Rev. E*, 62:3504–3507, Sep 2000.

[26] Iulia M Georgescu, Sahel Ashhab, and Franco Nori. Quantum simulation. *Reviews of Modern Physics*, 86(1):153, 2014.

[27] S Ghose, CR Paul, and R Stock. Quantum chaos and tunneling in the kicked top. *Laser physics*, 18(9):1098–1105, 2008.

[28] Shohini Ghose and Barry sanders. Entanglement dynamics in chaotic system. *Phys. Rev. A*, 70:062315, Dec 2004.

[29] Shohini Ghose, Rene Stock, Poul Jessen, Roshan Lal, and Andrew Silberfarb. Chaos, entanglement, and decoherence in the quantum kicked top. *Physical Review A*, 78(4):042318, 2008.

[30] Michael Grant and Stephen Boyd. Graph implementations for nonsmooth convex programs. In V. Blondel, S. Boyd, and H. Kimura, editors, *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008. http://stanford.edu/~boyd/graph_dcp.html.

[31] Michael Grant and Stephen Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. http://cvxr.com/cvx, March 2014.

[32] F. Haake, M. Kuś, and R. Scharf. Classical and quantum chaos for a kicked top. *Zeitschrift für Physik B Condensed Matter*, 65:381–395, 09 1987.

[33] Fritz Haake. Quantum signatures of chaos. In *Quantum Coherence in Mesoscopic Systems*, pages 583–595. Springer, 1991.

[34] Fritz Haake, M Kuś, and Rainer Scharf. Classical and quantum chaos for a kicked top. *Zeitschrift für Physik B Condensed Matter*, 65(3):381–395, 1987.

[35] Aram W Harrow. Applications of coherent classical communication and the schur transform to quantum information theory. *arXiv preprint quant-ph/0512255*, 2005.

[36] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[37] Melvyn Ho, Jean-Daniel Bancal, and Valerio Scarani. Device-independent certification of the teleportation of a qubit. *Physical Review A*, 88(5):052318, 2013.

[38] Melvyn Ho, Jean-Daniel Bancal, and Valerio Scarani. Device-independent certification of the teleportation of a qubit. *Phys. Rev. A*, 88:052318, Nov 2013.

[39] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60:1888–1898, Sep 1999.

[40] Anders Karlsson and Mohamed Bourennane. Quantum teleportation using three-particle entanglement. *Phys. Rev. A*, 58:4394–4400, Dec 1998.

[41] Karl Kraus, Arno Böhm, John D Dollard, and WH Wootters. States, effects, and operations: fundamental notions of quantum theory. lectures in mathematical physics at the university of texas at austin. *Lecture notes in physics*, 190, 1983.

[42] V. R. Krithika, V. S. Anjusha, Udaysinh T. Bhosale, and T. S. Mahesh. Nmr studies of quantum chaos in a two-qubit kicked top. *Phys. Rev. E*, 99:032219, Mar 2019.

[43] Meenu Kumari. Quantum-classical correspondence and entanglement in periodically driven spin systems. *Uwaterloo.ca*, 07 2019.

[44] Meenu Kumari and Shohini Ghose. Quantum-classical correspondence in the vicinity of periodic orbits. *Phys. Rev. E*, 97:052209, May 2018.

[45] Meenu Kumari and Shohini Ghose. Untangling entanglement and chaos. *Physical Review A*, 99(4):042311, 2019.

[46] S Leontica, F Tennie, and T Farrow. Simulating molecules on a cloud-based 5-qubit ibm-q universal quantum computer. *Communications Physics*, 4(1):1–7, 2021.

[47] Chi-Kwong Li and Diane Pelejo. Decomposition of quantum gates. *arXiv:1311.3599 [quant-ph]*, 12 2013.

[48] Jun Li, Ruihua Fan, Hengyan Wang, Bingtian Ye, Bei Zeng, Hui Zhai, Xinhua Peng, and Jiangfeng Du. Measuring out-of-time-order correlators on a nuclear magnetic resonance quantum simulator. *Physical Review X*, 7(3):031011, 2017.

[49] Xi-Han Li and Shohini Ghose. Control power in perfect controlled teleportation via partially entangled channels. *Phys. Rev. A*, 90:052305, Nov 2014.

[50] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, et al. Device-independent quantum random-number generation. *Nature*, 562(7728):548–551, 2018.

[51] Maurice Lombardi and Alex Matzkin. Entanglement and chaos in the kicked top. *Physical Review E*, 83(1):016207, 2011.

[52] Jian Ma, Xiaoguang Wang, C.P. Sun, and Franco Nori. Quantum spin squeezing. *Physics Reports*, 509:89–165, 12 2011.

[53] Vaibhav Madhok, Shruti Dogra, and Arul Lakshminarayan. Quantum correlations as probes of chaos and ergodicity. *Optics Communications*, 420:189–193, Aug 2018.

[54] Vaibhav Madhok, Vibhu Gupta, Denis-Alexandre Trottier, and Shohini Ghose. Signatures of chaos in the dynamics of quantum discord. *Phys. Rev. E*, 91:032906, Mar 2015.

[55] Lluis Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2(1):1–7, 2011.

[56] Eric J. Meier, Jackson Ang'ong'a, Fangzhao Alex An, and Bryce Gadway. Exploring quantum signatures of chaos on a floquet synthetic lattice. *Phys. Rev. A*, 100:013623, Jul 2019.

[57] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838–1840, Oct 1990.

[58] M. G. M. Moreno, Samuraí Brito, Ranieri V. Nery, and Rafael Chaves. Device-independent secret sharing and a stronger form of bell nonlocality. *Phys. Rev. A*, 101:052339, May 2020.

[59] C Neill, P Roushan, M Fang, Y Chen, M Kolodrubetz, Z Chen, A Megrant, R Barends, B Campbell, B Chiaro, et al. Ergodic dynamics and thermalization in an isolated quantum system. *Nature Physics*, 12(11):1037–1041, 2016.

[60] Yi-you Nie, Yuan-hua Li, Jun-chang Liu, and Ming-huang Sang. Quantum information splitting of an arbitrary three-qubit state by using two four-qubit cluster states. *Quantum Information Processing*, 10(3):297–305, 2011.

[61] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[62] Edward Ott. *Chaos in dynamical systems*. Cambridge university press, 2002.

[63] Asher Peres. *Quantum theory: concepts and methods*, volume 57. Springer Science & Business Media, 2006.

[64] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L Braunstein. Advances in quantum teleportation. *Nature photonics*, 9(10):641–652, 2015.

[65] Sandu Popescu. Bell's inequalities versus teleportation: What is nonlocality? *Phys. Rev. Lett.*, 72:797–799, Feb 1994.

[66] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[67] J M Radcliffe. Some properties of coherent spin states. *Journal of Physics A: General Physics*, 4:313–323, 05 1971.

[68] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, 2017.

[69] Bhaskar Roberts. Security analysis of quantum lightning. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 562–567. Springer, 2021.

[70] Joshua B Ruebeck, Jie Lin, and Arjendu K Pattanayak. Entanglement and its relationship to classical dynamics. *Physical Review E*, 95(6):062222, 2017.

[71] Vivek V Shende, Igor L Markov, and Stephen S Bullock. Minimal universal two-qubit controlled-not-based circuits. *Physical Review A*, 69(6):062321, 2004.

[72] George Svetlichny. Distinguishing three-body from two-body nonseparability by a bell-type inequality. *Phys. Rev. D*, 35:3066–3069, May 1987.

[73] Pascal Szriftgiser, Hans Lignier, Jean Ringot, Jean Claude Garreau, and Dominique Delande. Experimental study of quantum chaos with cold atoms. *Communications in Nonlinear Science and Numerical Simulation*, 8(3-4):301–313, 2003.

[74] IBM Quantum team. Retrieved from ibmq_vigo v1.0.2 (2020).

[75] B. F. Toner and D. Bacon. Communication cost of simulating bell correlations. *Phys. Rev. Lett.*, 91:187904, Oct 2003.

[76] Juha J Vartiainen, Mikko Möttönen, and Martti M Salomaa. Efficient decomposition of quantum gates. *Physical review letters*, 92(17):177902, 2004.

[77] Xiaoguang Wang, Shohini Ghose, Barry C Sanders, and Bambi Hu. Entanglement as a signature of quantum chaos. *Physical Review E*, 70(1):016217, 2004.

[78] Xiaoguang Wang, Shohini Ghose, Barry C Sanders, and Bambi Hu. Entanglement as a signature of quantum chaos. *Physical Review E*, 70(1):016217, 2004.

[79] John Watrous. *The theory of quantum information*. Cambridge University Press, 2018.

[80] William K Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80(10):2245, 1998.

[81] William K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245–2248, Mar 1998.

[82] Xiong Xu and Xiaoxue Wang. Controlled quantum teleportation via the ghz entangled ions in the ion-trapped system. *International Journal of Theoretical Physics*, 55(8):3551–3554, 2016.

[83] Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185–188, 2012.

[84] Hidehiro Yonezawa, Takao Aoki, and Akira Furusawa. Demonstration of a quantum teleportation network for continuous variables. *Nature*, 431(7007):430–433, 2004.

[85] Mark Zhandry. Quantum lightning never strikes the same state twice, 2017.

[86] Mark Zhandry. Quantum lightning never strikes the same state twice. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 408–438. Springer, 2019.

[87] Wojciech Hubert Zurek and Juan Pablo Paz. Quantum chaos: a decoherent definition. *Physica D: Nonlinear Phenomena*, 83(1-3):300–308, 1995.

APPENDICES

Appendix A

POVM and Projective Measurements

Quantum measurements are described by a set of operators $\{M_m\}$ acting on a quantum state ρ where m refers to the complete set of classical outcomes that may occur in the experiment. In every measurement one obtains only one of the possible outcomes m. The probability of getting the outcome m is given by:

$$P(m) = \mathrm{Tr}(\rho M_m) \tag{A.1}$$

The operators $\{M_m\}$ are called POVM(Positive Operator Valued Measurement). A POVM is characterized by the following properties:

$$M_m = M_m^\dagger \tag{A.2}$$

$$M_m \geq 0 \tag{A.3}$$

$$\sum_m M_m = \mathbb{I} \tag{A.4}$$

Projective measurements are a special case of $POVM$ measurements and are given by

$$\Pi_i = |\phi_i\rangle \langle\phi_i| \tag{A.5}$$

where $\{|\phi_i\rangle\}$ are a set of orthonormal basis states. It can be easily seen that Π_i satisfies Eq. (A.2) since $(|\phi_i\rangle \langle\phi_i|)^\dagger = |\phi_i\rangle \langle\phi_i|$. By the resolution of Identity into orthonormal basis, $\sum \Pi_i = \mathbb{I}$ thus satisfying Eq. (A.4). For any vector $|v\rangle$ in the space spanned by the orthonormal states $\{|\phi_i\rangle\}$, $\langle v|\phi_i\rangle \langle\phi_i|v\rangle = |\langle v|\phi_i\rangle|^2 \geq 0$, satisfying Eq. (A.3).

Appendix B

Semidefinite Programming

Given two Hilbert spaces $\mathcal{X}$ and $\mathcal{Y}$, let Φ be a Hermitian preserving map $T(\mathcal{X}, \mathcal{Y})$. Let $A \in \mathrm{Herm}(\mathcal{X})$ and $B \in \mathrm{Herm}(\mathcal{Y})$. A semidefinite program is a triple (Φ, A, B) with the following associated optimization problems [79, 23]:

$$\begin{array}{rr} \underline{\text{Primal problem}} & \underline{\text{Dual problem}} \\ \text{maximize:} \quad \langle A, X \rangle & \text{minimize:} \quad \langle B, Y \rangle \\ \text{subject to:} \quad \Phi(X) = B & \text{subject to:} \quad \Phi^\dagger(Y) \succeq A \\ X \in Pos(\mathcal{X}) & Y \in Herm(\mathcal{Y}) \end{array} \tag{B.1}$$

Where $\Phi^\dagger$ is the adjoint of Φ specified by the unique map satisfying $\langle Y, \Phi(X) \rangle = \langle \Phi^\dagger(Y), X \rangle$ for every $X \in \mathrm{L}(\mathcal{X})$ and $Y \in \mathrm{L}(\mathcal{Y})$. We define $\mathcal{A} = \{X \in \mathrm{Pos}(\mathcal{X}) \mid \Phi(X) = B\}$ and $\mathcal{B} = \left\{Y \in \mathrm{Herm}(\mathcal{Y}) \mid \Phi^\dagger(Y) \succeq A\right\}$. $\mathcal{A}$ and $\mathcal{B}$ are *feasible sets* of the *primal problem* and *dual problem*, respectively. The *optimal values* of the primal and dual problems are denoted by $\alpha = \sup\{\langle A, X \rangle : X \in \mathcal{A}\}$ and $\beta = \inf\{\langle B, Y \rangle : Y \in \mathcal{B}\}$ respectively. By *weak duality* $\alpha \geq \beta$. *Strong duality* holds when $\alpha = \beta$. A sufficient condition of strong duality is given by the *Slater's condition*:

Theorem 2. *For a semidefinite program (Φ, A, B), if $\mathcal{A} \neq \emptyset$ and there exists a $Y \in \mathrm{Herm}(\mathcal{Y})$ which strictly satisfies the dual problem, i.e., $\Phi^\dagger(Y) \succ A$, then $\alpha = \beta$ and the optimal value is obtained in the primal problem.*

Now consider the optimization program given in Eq. (3.27). We can cast it into a semidefinite program in the following way:

Let $\mathcal{X}$ be a Hilbert space of dimension D, where D is also the dimension of Derek's quantum system. $\Phi \in T(\mathcal{X}, \mathcal{X})$. Then the optimization problem is given by:

$$\begin{array}{rll} & \underline{\text{Primal problem}} & \underline{\text{Dual problem}} \\ \text{maximize:} & \langle(\tilde{\rho_1}, \tilde{\rho_2}, ..., \tilde{\rho_n}), (M_1, M_2, ..., M_n)\rangle & \text{minimize:} \quad \langle \mathbb{I}_D, Y \rangle \\ \text{subject to:} & \Phi(M_1, M_2, ..., M_n) \triangleq \sum_{i=1}^{n} M_i = \mathbb{I}_D & \text{subject to:} \quad \Phi^\dagger(Y) \succeq (\tilde{\rho_1}, \tilde{\rho_2}, ..., \tilde{\rho_n}) \\ & (M_1, M_2, ..., M_n) \in \text{Pos}(\mathcal{X})^n & Y \in \text{Herm}(\mathcal{X}) \end{array} \tag{B.2}$$