Background: Quantum teleportation is a communication method in which the state of a quantum system at one point in space can be reconstructed at another using pre-shared entanglement (an EPR Pair) and classical communication [1]. A crucial application of teleportation is distributed quantum computation: by teleporting quantum systems between distributed parties, an arbitrary quantum circuit can be divided into parts and implemented across potentially large distances. One drawback of using the standard teleportation protocol for distributed computation is that it requires exchanging classical communication at each computational step. This makes distributed quantum computation using standard teleportation infeasible for near-term quantum hardware, which lacks the ability to store quantum information for extended periods of time. Because the speed of communication is bounded by the speed of light c, each round of communication in a teleportation protocol will require a time length of at least $\Delta t = d/c$, where d is the distance between separated parties. The fact that distributed computation requires a minimum amount of time to perform can be **exploited for cryptographic purposes**.

For example, quantum position verification (QPV) is a task in which an untrusted agent, P, attempts to prove her geographical position to verifiers ($V_0, V_1, \ldots, V_n$) by performing a given computation within a bounded timeframe [2]. To illustrate, in the simplest QPV protocol with two verifiers, V_0 prepares and sends a quantum bit (qubit) $|\phi\rangle$ in one of four states to P: the states of the computational basis $|0\rangle$ or $|1\rangle$, or the states of the Hadamard basis $|+\rangle$ or $|-\rangle$. V_1 transmits the basis θ in which to measure the qubit to the untrusted agent P, and the actions of the verifiers are timed such that the qubit and basis information arrive at the location of the agent at the same time. If the agent P is not at the purported location, then it will take her too long to receive the input data, perform the computation, and return the outcome to the honest verifiers.

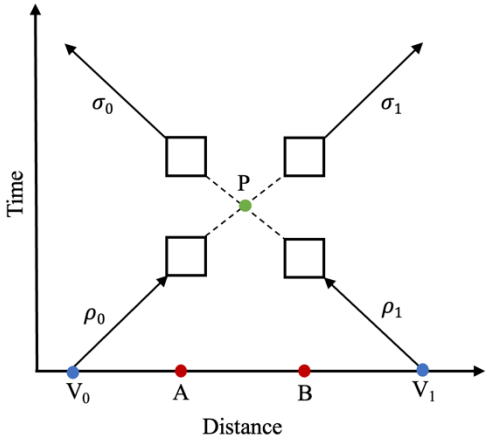

Figure 1: Adversaries, Alice and Bob, attack a general protocol for position verification, attempting to simulate the action of an agent P at the claimed location. The attackers respond to the messages ρ_0 from V_0 and ρ_1 from V_1 with σ_0 and σ_1. They have time for a single round of simultaneous communication.

A group of adversaries can attack this protocol by performing the same computation in a distributed manner, such that none of them are truly located at the spatial coordinate being certified. However, to achieve a successful attack in the allowed time frame, the adversaries can only perform a single round of simultaneous communication [2]. This distributed computation performed using just one round of communication and pre-shared entanglement is often called **non-local quantum computation** (NLQC) [3]. Despite its **significance to quantum cryptography and quantum communication** in general, the limitations and possibilities of NLQC are largely unknown, especially for more than two parties. *This research proposes to determine the entanglement cost for performing NLQC by constructing new one-round teleportation protocols and discovering connections between NLQC and cryptographic primitives like QPV.*

Identified Capability Gap: In a general NLQC protocol, the separated parties have some pre-shared entanglement, and given some input data, they use their entanglement plus one round of communication to perform the desired computation on the input. A fundamental question is *how much entanglement* is required by the parties to perform a specific computation. The initial major

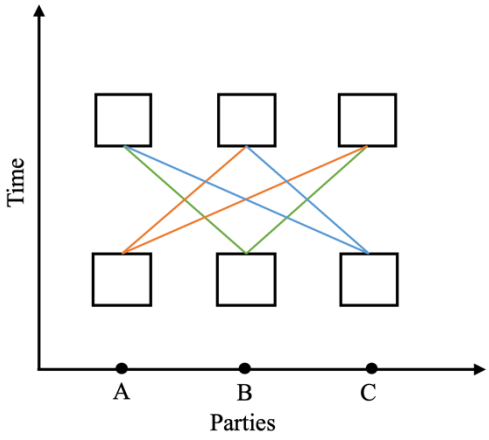

Figure 2: NLQC with k = 3 parties sharing an entangled quantum

result to this question was provided by Vaidman, who showed that NLQC is universal [3]: every quantum computation can be performed to arbitrarily high precision using NLQC and a sufficiently large amount of entanglement. The cost of entanglement in Vaidman's original protocol, however, grows double exponentially with the dimension of the input systems. An improvement on this scheme was later made using port-based teleportation [4], which reduced the entanglement cost to just being exponential in size. Determining whether sub-exponential universal NLQC protocols exist remains a major open problem – one I intend to solve.

When considering cryptographic applications such as QPV, the entanglement cost for performing NLQC quantifies how much entanglement is needed by adversaries to break the security. The task of QPV and its connection to NLQC has been noted above. It has been recognized very recently, however, that **NLQC also plays a fundamental role in other cryptographic schemes**. A special case of NLQC known as *f*-routing was recently proven to be equivalent to the quantum generalization of a cryptographic primitive known as conditional disclosure of secrets (CDS). Additionally, deep connections between secret sharing (SS) and QPV have been identified: SS giving CDS with the same efficiencies is an existing relation among the primitives, and the classical CDS scheme was shown to imply a similarly efficient quantum CDS scheme using a one-time pad. It has also been shown that a special case of NLQC known as coherent function evaluation (CFE) induces efficient private simultaneous message passing (PSM) protocol using quantum resources [5].

CDS and PSM generally involve k parties; but only the case of $k = 2$ has been related to non-local computation so far. These results reveal that NLQC is an important operational model to consider for quantum cryptography, and its full capabilities should be understood, especially for $k > 2$ parties. This research will work towards **finding new upper and lower bounds on the entanglement cost for performing NLQC.** The upper bounds will provide specific attacks that adversaries could use in cryptographic applications, while the lower bounds will establish security thresholds, describing how much entanglement the adversaries will need to break a given cryptographic protocol. A prized goal would be to prove exponential lower bounds, implying the scheme is secure against any practical attack.

Proposed Methodology: This research aims to study entanglement cost for multi-partite NLQC by attacking the problem in two directions: computing the upper and lower bounds. I plan to conduct this research in the Quantum Information Group at UIUC under Professor Eric Chitambar.

Upper Bounds*:* For my proposed work, I will explore new teleportation protocols that are optimized for performing different quantum computations. A particular technique we will study and generalize for identifying new protocols is the garden-hose model of computation. In the garden-hose model, there are many pipes connecting two parties, Alice and Bob. For a given Boolean function $f:\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ and inputs (x, y), the parties locally connect their pipes together in such a way that the water flows to Alice if $f(x, y) = 0$ and it flows to Bob if $f(x, y) = 1$ [6]. In its application to NLQC, every pipe represents an EPR pair and each strategy of how the players locally connect their pipes exemplifies a different teleportation protocol. I will extend this computational model with the addition of Carol, such that Bob is now an intermediate agent between Alice and Carol, and the inputs of (x, y, z). Bob connects the pipes of Alice and

Carol so that if $f(x, y, z) = 0$, the water flows to Alice and if $f(x, y, z) = 1$, the water flows to Carol. This setup will enable me to define and study the "garden hose complexity" for general multipartite functions, analogous to the complexity analysis conducted under the bipartite garden hose model [6]. Through the additional parties, I will build upon the garden hose model to construct NLQC protocol for $k > 2$ parties.

As an additional approach to determine entanglement upper bounds in NLQC, I will examine the possibility of transforming different quantum computation models into non-local schemes. For example, there are known methods for translating a given quantum circuit into a teleportation-based NLQC protocol based on the T-gate structure of the circuit [6]. However, there are other universal quantum computational paradigms to consider here beyond Pauli + T-gates, such as qudit quantum computation, matchgate computation, and measurement-based quantum computing. I aim to investigate how a quantum computing circuit, algorithm, or protocol in one of these other models can be translated into a corresponding NLQC protocol. Potentially less entanglement will be needed in these protocols.

Lower Bounds*:* Previous work has shown that in the bipartite case, the classical cryptographic primitives of CDS and PSM are related to NLQC [5]. I will apply a similar method and explore whether multi-partite classical cryptography protocols, such as secret sharing (SS) and key agreement, can be connected to NLQC. When $k = 2$, it has been shown that any distributed CDS protocol using pre-shared entanglement can be transformed into a NLQC scheme using the same amount of entanglement. Hence, lower bounds on CDS translate to lower bounds on NLQC. I will evaluate whether a similar reduction can be shown for a multi-partite version of CDS, and whether cryptographic reductions like this can be used to lower bound the entanglement cost of NLQC. In the case of two parties, the canonical entangled state $1/\sqrt{2}(|00\rangle + |11\rangle)$ is the key resource in performing NLQC. However, when moving to more parties, different types of entangled states could be useful, such as the GHZ state $1/\sqrt{2}(|000\rangle + |111\rangle)$ or the W-state $1/\sqrt{3}(|100\rangle + |010\rangle + |001\rangle)$. To prove both lower and upper bounds in my study of multi-party NLQC, I will likely need to use consider the different properties of multi-party entangled states and their advantages/disadvantages in distributed computation.

Motivation and Impact: The research proposed here directly aligns with the **Quantum Information Technology goal of the ONR**, as well as the **Information and Networks and Physical Sciences areas of the AFOSR** – particularly the **Quantum Information Sciences, and Information Assurance and Cybersecurity sections**. This work will focus on understanding and exploiting non-classical physical resources for the development of capabilities beyond those currently possible with classical systems in the areas of **networking and communications** and **information processing**. **Quantum resources**, such as entanglement and non-locality, and **quantum communication complexity** are **crucial to the security of future communication and computing systems**, in which classical and quantum devices interact. This research will impact the defense against and prevention of cyberattacks and offer potentially unparalleled solutions to current or future problems.

My previous work in quantum systems and classical cybersecurity has provided me with an excellent foundation to study quantum networks and the enhanced security offered by quantum information processing. Because the protocols studied in this proposed work require few qubits, **near-term implementation is feasible**. Consequently, this research will contribute towards active research projects at the Illinois Quantum Information Science and Technology Center (IQUIST) Center at UIUC and lead to experimental collaborations and help to grow the local testbed by providing realistic new use-cases and cryptographic protocols for quantum networks.

References:

[1] Charles H. Bennett, Gilles Brassard, Claude Crepeau, 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. doi:10.1103/PhysRevLett.70.1895.

[2] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. SIAM Journal on Computing, 43(1):150–178, January 2014. doi:10.1137/130913687. URL https://doi.org/10.1137/130913687.

[3] Lev Vaidman. Instantaneous measurement of nonlocal variables. Phys. Rev. Lett., 90:010402, Jan 2003.doi:10.1103/PhysRevLett.90.010402.

[4] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. New Journal of Physics, 13(9):093036, September 2011. doi:10.1088/1367-2630/13/9/093036. URL https://doi.org/10.1088/1367-2630/13/9/093036.

[**5]** Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography, 2023.

[6] Florian Speelman. Instantaneous non-local computation of low t-depth quantum circuits. 2016. doi:10.4230/LIPICS.TQC.2016.9. URL http://drops.dagstuhl.de/opus/volltexte/2016/6690/.