Project Specification: Interactive Proofs for Resource-Constrained Quantum Learning

Alex Do

Supervised by Dr Matthias Caro
3rd Year of Study
Department of Computer Science, University of Warwick

Abstract

Interactive proofs for quantum learning represent a promising frontier for enabling secure delegation of quantum machine learning tasks to untrusted quantum servers. However, practical deployment of these protocols faces significant challenges when operating under realistic resource constraints, including limited quantum memory, finite coherence times, and restricted communication bandwidth. This project explores the development and optimization of resource-efficient interactive verification protocols that can operate effectively within the constraints of near-term quantum devices. The first objective is to design and analyze modified interactive proof systems that minimize quantum resource requirements while maintaining security guarantees, focusing on protocols that can accommodate noisy hardware limitations and decoherence effects. The second goal involves developing protocols that can dynamically adapt to varying decoherence levels in available quantum hardware, potentially adjusting verification strategies based on theoretical assessment of device coherence properties. This work aims to bridge the gap between the theoretical promise of quantum learning verification and its practical applicability on resource-constrained quantum systems, potentially enabling broader adoption of verified quantum machine learning in real-world applications.

Acknowledgements

I would like to thank Edmund Goodman, a now-Warwick-grad and current student at the University of Cambridge for Advanced Computer Science, for permission to use his title page design. I would also like to thank Dr. Matthias Caro for helping me throughout the ideation stages of this specification.

Contents

Chapter 1

Introduction

The field of quantum computing is predicated on the potential to solve certain computational problems that are believed to be intractable for even the most powerful classical computers. This promise of "quantum advantage" extends to machine learning, where quantum algorithms may offer exponential speedups in tasks such as data classification [RML14], representational power [Pir+23], and runtimes for learning and inference [GZD18].

1.1 Problem Statement

The physical realization of large-scale, fault-tolerant quantum computers that we have seen flourish with classical computers still remains a formidable scientific and egineering challenge. In the forseeable future, access to these powerful devices will likely be limited, provided primarily through cloud-based platforms where users remotely submit computational tasks to a quantum server and can verify classically its computation [MN20].

The trust issue inherent in the client-server model is what necessitates interactive proofs - the client acts as the "verifier" and the server as the "prover". The goal is for the computationally weak client to verify the result from the powerful, but untrusted server.

This culminated in the discovery of Mahadev's breakthrough verification protocol [Mah23], where she was able to achieve a strong result centred around the Quantum Prover Interactive Proof (QPIP) [Aha+17]. She found that under some preconditions, all decision problems which can efficiently be computed in quantum polynomial time (BQP) can be verified by an efficient classical machine through interaction.

Quantum learning is a key application for this model - reliable schemes that allow classical clients to delegate learning to untrusted quantum servers is a prerequisite to having widespread access to quantum learning advantages, with [Car+24] extending the notion of interactive proofs to also apply to quantum learning problems originally started by [Gol+21].

1.2 Research Gap

A significant gap exists between the theoretical promise of verification and its practical feasibility. While recent research has demonstrated that purely classical clients can verify highly structured learning problems (such as agnostic parity learning), even on noisy quantum hardware [MSD24], these solutions are not broadly generalizable. For a wider class of quantum learning tasks, it has been shown that classical interaction is fundamentally insufficient for a resource-constrained verifier to overcome their limitations [Car+25].

The central challenge is therefore to make targeted optimizations on existing verification schemes, surgically reducing their demands on critical resources from client memory, communication bandwidth, to coherence times. I aim to do this whilst building in robustness against noise and decoherence effects, bridging an implementation gap and modifying a protocol to operate effectively within realistic constraints to find a concrete path toward making secure, delegated QML a practical reality on the hardware of the near future.

Chapter 2

Objectives

These objectives will be cleanly divided into core work required to produce a complete dissertation within a 6-month timeframe, followed by a rough outline of follow-up work time-permitting.

2.1 Must-have Objectives

2.1.1 Foundational Literature Review and Protocol Selection

Initially, I will conduct a thorough, focussed literature review ([Car+24], [Car+25], [Mah23] and related and cited works) to map the landscape of interactive proofs for quantum learning. This will identify and summarize foundational protocols, and more importantly, analyze recent, resource-efficient proposals designed for near-term application.

A strong candidate ([MSD24], for example) would be a protocol with a classical verifier or one that explicitly addresses noise - this should approximatly occupy the first month of work.

2.1.2 Theoretical Analysis of the Selected Protocol

Once a protocol is selected, I will perform a detailed theoretical investigation and analysis of its components and resource requirements under ideal conditions, breaking down the protocol into its constituent steps and quantifying computational loads. This will include runtime complexity, (quantum) memory overhead, and the magnitude of data communicated over its channel.

2.1.3 Simulation and Performance Analysis under a Realistic Noise Model

This is the main practical component of the project, implementing a simplified, small-scale version of a previously unimplemented protocol (for example the recent work from Caro et. al. [Car+24]). I will then introduce a standard noise model to the simulation, the goal being to run experiments that measure how the protocol's key properties (completeness and soundness) degrade as noise increases. This should also occupy a month of time.

One method of noise generation I could explore is the depolarizing channel [Kin02], also implemented by `PennyLane` [Pen25].

2.1.4 Proposing and Simulating a Protocol Modification

Based on insights from simulation and theoretical analysis, I will propose a series of modifications to the protocol aimed at improving its noise tolerance or resource efficiency. I will then both prove its validity theoretically when appropriate and through simulation too. I estimate this will take around 3 months.

2.2 Could-have Objective

2.2.1 Theoretical Framework for an Adaptive Protocol

Finally, as a path of extension, I will aim to develop an adaptive protocol which can alter its parameters or behaviour based on network conditions. This could be from a purely theoretical or potentially more practical standpoint. This will take around 3 months, generously, but I will be able to write about it before completion from a development standpoint if uncompleted.

Chapter 3

Methods & Methodologies

This project will adopt a multi-stage, mixed-methods approach that combines systematic literature review, theoretical analysis, and computational simulation. The method is designed to establish a firm understanding of the current research landscape and then deconstruct a (or several) key protocol(s) to analyze its theoretical properties and practical viability.

The project will be managed through a structured and phased research plan with clearly defined milestones. This ensures it remains on track within the six-month period of the dissertation scope whilst leaving room for adaptability further down the timeline.

Aligning tightly with the objectives set out in chapter 2, we outline a few key phases:

1. Foundational Literature Review

2. Analysis and Implementation of the Selected Protocol

3. Designing Modifications for the Selected Protocol

The primary method of literature review will be a targeted search of academic databases, including arXiv [Uni25], Google Scholar [Goo25], and the American Physical Society [Soc25]. The review will predominantly focus on foundational papers containing keywords such as ”interactive proofs”, ”verifiable quantum learning”, ”delegated quantum learning/computation” that establish a client-server model for quantum computation and more specifically, learning, before narrowing to more recent proposals that explicilty aim to minimize verifier resources or tolerate noise.

Following the literature review, the project will move in the direction of rigorous theoretical and practical analysis. This will involve decomposing a protocol into fundamental components - the roles of the verifier and prover, the required quantum and classical resources for each party, the communication flow, and security guarantees (completeness and soundness defined in the definition of QPIP [Aha+17]). The practical analysis will predominantly involve the implementation of a previously unimplemented verification protocol, which we will build with a widely-supported quantum computing framework such as IBM’s Qiskit [Jav+24]. We will execute the implementation in both ideal, noise-free environments as well as with standard noise models [GEZ21]. With this, we will be able to compute metrics including the protocol’s completeness and soundness from a practical methodology.

Based on the insights gathered from the previous phase, the final phase will focus on designing and evaluating targeted modifications to a selected protocol, transitioning from analysis to synthesis with a tangible improvement that enhances the protocol's robustness and resource-efficiency. The proposed modifications will be implemented within the existing Qiskit simulation framework to allow for a direct and controlled comparison, with a modification being considered successful if it demonstrates a statistically significant improvement in noise resilience compared to its initial implementation.

Chapter 4

Timetable

Table 4.1: Project Timetable

Week	**Event / Task**
Summer – T1 W1	Initiation of project. Background reading on quantum computing and interactive proof systems with use cases.
T1 W2	Submission of project specification document.
T1 W3–W6	Complete a thorough, focussed literature review to map the landscape of interactive proofs for quantum learning, including in noisy environments.
T1 W7–W8	Investigate and select the strongest candidate protocol with a classical verifier for both theoretical and practical analysis.
T1 W9	Submission of progress report.
T1 W9–W10	Perform detailed theoretical analysis over the selected protocol
Christmas Holidays	Perform detailed simulation and performance analysis over several realistic noise models for the chosen protocol.
T2 W1	Begin theorizing potential protocol modifications.
T2 W2–W6	Theoretically and practically analyze a series of candidate modifications.
T2 W6-W8	Iterate and improve on previous results. Collect data.
T2 W9	Submission of mid-term progress presentation.
T2 W10	Verify all results.
Easter Holidays	Optional exploration of new protocols. Complete final report.
T3 W1	Submission of final report.

Chapter 5

Resources & Risks

This project will primarily rely on standard software and accessible high-performance computing hardware owned by the Department of Computer Science. In particular, I refer to the DCS Batch Compute system for more intensive simulations, especially those leveraging noise models mentioned earlier [Kin02].

For initial development and small-scale simulations, I will perform these on a personal Macbook M3 Pro. I will also leverage free cloud-based access to real quantum hardware provided by IBM [IBM25], which at the time of writing grants open-plan users a set amount of free execution time on their devices per month to run small-scale onstances of the selected protocol on real Noisy Intermediate-Scale Quantum (NISQ) devices. This will offer a valuable insight into the difference between simulated noise models and real-world hardware performance. It is possible that IBM revokes access to their real NISQ devices for free, but it is only a nice-to-have of the project rather than its central focus - therefore not a large risk.

A number of books and and papers will also be reviewed throughout the course of this project ([Car+24], [Car+25], [Aha+17], to begin with) but all materials used in future will be properly referenced in the following reports. I will also keep regular, biweekly communication going with my supervisor, Dr. Matthias Caro, as well as get in touch other students in the field.

It is also possible that finding changes to make to quantum protocols becomes infeasible after thorough investigation (possibly due to mathematical or practical complexity). In this case, I will be able to back up the conclusion with empirical and theoretical evidence of work, as well as contribute a larger number of implementations on quantum interactive proof protocols that have not yet been explored.

Chapter 6

Legal, Social, Ethical and Professional Issues & Considerations

As this project is largely theoretical in nature, involving literature review and computational simulation, it does not directly engage with sensitive personal data or human subjects. The primary professional considerations are therefore centred on academic integrity and responsible research conduct. This includes the rigorous and honest reporting of simulation results, transparently acknowledging the limitations of noise models used, and providing proper attribution to all sources and libraries used in accordance with their open-source licenses. The project will be conducted entirely within the ethical and professional guidelines set by the Department of Computer Science of the University of Warwick.

However, the research area of delegated quantum computing underpinning this project is deeply connected to significant legal, social, and ethical considerations. Whilst this work aims to make Quantum Machine Learning more practical, it touches upon the well-established ethical concerns of algorithmic bias and fairness. Whilst verifying computational correctness is distinct from verifying fairnes, it is a professional responsibility to acknowledge that any technology enabling powerful machine learning models must eventually be paired with governance to prevent inequitable outcomes.

Bibliography

[Aha+17] Dorit Aharonov et al. *Interactive Proofs for Quantum Computations.* 2017. arXiv: 1704.04487 [quant-ph]. URL: https://arxiv.org/abs/1704.04487.

[Car+24] Matthias C. Caro et al. "Classical Verification of Quantum Learning". en. In: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. DOI: 10.4230/LIPICS.ITCS.2024.24. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2024.24.

[Car+25] Matthias C. Caro et al. *Interactive proofs for verifying (quantum) learning and testing.* 2025. arXiv: 2410.23969 [quant-ph]. URL: https://arxiv.org/abs/2410.23969.

[GEZ21] Konstantinos Georgopoulos, Clive Emary, and Paolo Zuliani. "Modeling and simulating the noisy behavior of near-term quantum computers". In: *Physical Review A* 104.6 (Dec. 2021). ISSN: 2469-9934. DOI: 10.1103/physreva.104.062432. URL: http://dx.doi.org/10.1103/PhysRevA.104.062432.

[Gol+21] Shafi Goldwasser et al. "Interactive Proofs for Verifying Machine Learning". In: *12th Innovations in Theoretical Computer Science Conference (ITCS 2021).* Ed. by James R. Lee. Vol. 185. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 41:1–41:19. ISBN: 978-3-95977-177-1. DOI: 10.4230/LIPIcs.ITCS.2021.41. URL: https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2021.41.

[Goo25] Google. 2025. URL: https://scholar.google.com/ (visited on 10/14/2025).

[GZD18] X. Gao, Z.-Y. Zhang, and L.-M. Duan. "A quantum machine learning algorithm based on generative models". In: *Science Advances* 4.12 (2018), eaat9004. DOI: 10.1126/sciadv.aat9004. eprint: https://www.science.org/doi/pdf/10.1126/sciadv.aat9004. URL: https://www.science.org/doi/abs/10.1126/sciadv.aat9004.

[IBM25] IBM. 2025. URL: https://www.aps.org/publications (visited on 10/14/2025).

[Jav+24] Ali Javadi-Abhari et al. *Quantum computing with Qiskit.* 2024. DOI: 10.48550/arXiv.2405.08810. arXiv: 2405.08810 [quant-ph].

[Kin02] C. King. *The capacity of the quantum depolarizing channel.* 2002. arXiv: quant-ph/0204172 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/0204172.

[Mah23] Urmila Mahadev. *Classical Verification of Quantum Computations*. 2023. arXiv: 1804.01082 [quant-ph]. URL: https://arxiv.org/abs/1804.01082.

[MN20] Tomoyuki Morimae and Harumichi Nishimura. *Rational proofs for quantum computing*. 2020. arXiv: 1804.08868 [quant-ph]. URL: https://arxiv.org/abs/1804.08868.

[MSD24] Yinghao Ma, Jiaxi Su, and Dong-Ling Deng. *Classical Verification of Quantum Learning Advantages with Noises*. 2024. arXiv: 2411.09210 [quant-ph]. URL: https://arxiv.org/abs/2411.09210.

[Pen25] PennyLane. 2025. URL: https://docs.pennylane.ai/en/stable/code/api/pennylane.DepolarizingChannel.html (visited on 10/16/2025).

[Pir+23] Niklas Pirnay et al. "Superpolynomial quantum-classical separation for density modeling". In: *Physical Review A* 107.4 (Apr. 2023). ISSN: 2469-9934. DOI: 10.1103/physreva.107.042416. URL: http://dx.doi.org/10.1103/PhysRevA.107.042416.

[RML14] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd. "Quantum Support Vector Machine for Big Data Classification". In: *Physical Review Letters* 113.13 (Sept. 2014). ISSN: 1079-7114. DOI: 10.1103/physrevlett.113.130503. URL: http://dx.doi.org/10.1103/PhysRevLett.113.130503.

[Soc25] American Physical Society. 2025. URL: https://www.aps.org/publications (visited on 10/14/2025).

[Uni25] Cornell University. 2025. URL: https://arxiv.org/ (visited on 10/14/2025).