The quantum internet: Verification of quantum computation

(Dated: April 20, 2017)

I. INTRODUCTION

A. Relevance of verification of quantum computation for the quantum internet

Adversarial settings for non-NP problems...etc

B. Definition of verification

Mention the algorithms this is relevant for (e.g., *not* NP)

C. Relationship to other kinds of verification

Hypothesis testing; self-analysis; randomised bench-marking; state certification; authentication (ask Si-Hui)

II. VERIFICATION OF UNIVERSAL QUANTUM COMPUTATION

Also mention relationship to blind quantum computation: only 2 examples of verifiable computing schemes that are not naturally blind

A. Two-party verification

1. MBQC and traps

2. Measurement-only verification

Also mention relationship to state certification

3. Multi-party verification

III. VERIFICATION OF NON-UNIVERSAL MODELS

List non-universal models

A. Verification of quantum simulation

B. DQC1

C. Boson sampling

Circumstantial tests;

D. IQP

Michael Bremner, Jozsa, Shepherd: sampling problem; Also Bremner (lattice model?)

E. Others

IV. FURTHER WORK

A. Continuous variables

Example: advantage of measurement-only scheme: can be extended to an arbitrary size network and security of any one party is not compromised. Note also that a quantum software program is a particular quantum state that enables a quantum computer to perform a specific task (Preskill). So might think of the cubic states as a kind of quantum program? Consider the scenario that every downloaded state costs something.

B. Verification and quantum machine learning algorithms

C. Security in distributed computing