Quantum Internet Alliance M4.2: List of atomic tasks

H. Ollivier

2020-02-24

1 Purpose

Application level protocols need to have access to networking services such as entanglement sharing between any two points of the network. While such service is at the heart of the quantum internet architecture, additionnal functionalities can be requiered or just convenient to have for better, faster, wider development of application level protocols.

The purpose of this report is to review a wide range of such protocols searching for atomic repeatable functions while categorising them along several dimensions (such as their corresponding network stage). By doing so, we aim at providing building blocks that would:

- lessen the amount of code and control needed while developing applications;
- allow benchmarking of the nodes and network capabilities against these tasks;
- provide functionalities with sound cryptographic definitions;
- provide a simulation platform where these functions would already be implemented, to further accelerate the creation cycle of a quantum protocols, as well as providing reusability of code.

2 Methodology

1. Review of the entire quantum protocol zoo looking at each protocol;
2. Identification and grouping of candidate atomic functions;

3. Categorising various candidates into network stages, type (quantum internet layer attribution, off-layer), and necessity

4. Integration into protocol zoo's knowledge graph

3 Review of the quantum protocol zoo

Protocol	Atomic Function Candidates
GHZ-based Quantum Anonymous Transmission https://arxiv.org/abs/quant-ph/0409201	Classical authenticated chan GHZ creation and broadcast Classical collision detection Single qubit measurement Single qubit Hadamard gate Limited memory Teleportation
Verifiable Quantum Anonymous Transmission https://arxiv.org/pdf/1811.04729.pdf	Notification (private comput Single qubit measurements i Imperfect GHZ source Limited memory (Uses GHZ anonymous tran
Polynomial Code based Quantum Authentication https://arxiv.org/pdf/quant-ph/0205128.pdf	Clifford circuits (error corre Memory
Fast Quantum Byzantine Agreement https://dl.acm.org/doi/10.1145/1060590.1060662	Distribution of GHZ state a Verification of n-party maxi (Uses oblivious common coi (Uses verifiable QSS)
Quantum Bit Commitment https://arxiv.org/abs/1108.2879	BB84 encoding of classical i Single qubit measurement in Secure classical channel Fast operations to keep the
Quantum Coin Flipping https://arxiv.org/abs/quant-ph/9904078	$\pi/9$ single qubit preparation Multi qubit POVM
Gottesman and Chuang Quantum Digital Signature https://arxiv.org/abs/quant-ph/0105032	Memory Swap test Stabilizer states creation
Prepare and Measure Quantum Digital Signature (QDS)	Quantum authenticated cha BB84 encoding BB84 decoding
Measurement Device Independent QDS	Classical authenticated chan Measurement Device Indepe BB8484 Encoding and Deco
Multipartite Entanglement Verification	Authenticated classical chan Secure classical broadcast Common shared randomness Limited memory BB84 Measurements GHZ source / broadcast
Quantum Fingerprinting	Clifford gates Swap test
BB84	BB84 Encoding and Decodi Authenticated classical chan Privacy amplification Information reconciliation
Device Independent QKD	EPR distribution Information reconciliation

4 Task extraction and categorisation

Function	Layer	TN
Sending qubit	Transport / Session	
Sending qubit blocks	Transport / Session	
BB84 Encoding	Presentation	
BB84 Decoding	Presentation	
Quantum One Time Pad / confidential channel (encoding and decoding)	Session	
Classical authenticated channel	Off	
Creation and braodcast of GHZ state	Network	
Creation and broadcast of any stabilizer state	Network	
Creation and broadcast of arbitrary graph states	Network	
Single Qubit Measurement in equatorial plane	Presentation	
Local Pauli gates	Off	
Local Clifford gates	Off	
Local memory	Off	
Non Cliffort gates	Off	
Anonymous transmission channel	Transport / Session	
Teleportation protocol	Transport	
Verification of stabilizer state	Off	
(V)QSS	Off	
Quatum authenticated channel	Transport / Session	
QFactory	Off	
Equatorial states preparation (local) arbitrary angle or given set	Off	
Swap Test	Off	
Multi qubit POVM	Presentation	
Privacy amplification	Off	
Information reconciliation	Off	
Secure classical broadcast channel	Tranport / Session	
Common Shared Randomness	Off	
Weak Coin Flipping	Application	
Quantum 1 way function	Off	