Quantum Internet Alliance M4.2: List of atomic tasks

H. Ollivier

2020-02-24

# 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.

# 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

# Review of the quantum protocol zoo

|  |  |
| --- | --- |
| Protocol | Atomic Function Candidates |
| GHZ-based Quantum Anonymous Transmission | Classical authenticated channels |
| <https://arxiv.org/abs/quant-ph/0409201> | GHZ creation and broadcast |
|  | Classical collision detection protocol |
|  | Single qubit measurement |
|  | Single qubit Hadamard gate |
|  | Limited memory |
|  | Teleportation |
| Verifiable Quantum Anonymous Transmission | Notification (private computation of classical parity, OR, Rand) |
| <https://arxiv.org/pdf/1811.04729.pdf> | Single qubit measurements in the equatorial plane |
|  | Imperfect GHZ source |
|  | Limited memory |
|  | (Uses GHZ anonymous transmission as subroutine) |
| Polynomial Code based Quantum Authentication | Clifford circuits (error correction) |
| <https://arxiv.org/pdf/quant-ph/0205128.pdf> | Memory |
| Fast Quantum Byzantine Agreement | Distribution of GHZ state among n parties |
| <https://dl.acm.org/doi/10.1145/1060590.1060662> | Verification of n-party maximally entangled state |
|  | (Uses oblivious common coin) |
|  | (Uses verifiable QSS) |
| Quantum Bit Commitment | BB84 encoding of classical information |
| <https://arxiv.org/abs/1108.2879> | Single qubit measurement in computational and +/- bases |
|  | Secure classical channel |
|  | Fast operations to keep the relativistic constraints |
| Quantum Coin Flipping | single qubit preparation |
| <https://arxiv.org/abs/quant-ph/9904078> | Multi qubit POVM |
| Gottesman and Chuang Quantum Digital Signature | Memory |
| <https://arxiv.org/abs/quant-ph/0105032> | Swap test |
|  | Stabilizer states creation |
| Prepare and Measure Quantum Digital Signature (QDS) | Quantum authenticated channel (unfortunately stronger than QDS) |
|  | BB84 encoding |
|  | BB84 decoding |
| Measurement Device Independent QDS | Classical authenticated channels |
|  | Measurement Device Independent QKD link |
|  | BB8484 Encoding and Decoding |
| Multipartite Entanglement Verification | Authenticated classical channels |
|  | Secure classical broadcast |
|  | Common shared randomness |
|  | Limited memory |
|  | BB84 Measurements |
|  | GHZ source / broadcast |
| Quantum Fingerprinting | Clifford gates |
|  | Swap test |
| BB84 | BB84 Encoding and Decoding |
|  | Authenticated classical channel |
|  | Privacy amplification |
|  | Information reconciliation |
| Device Independent QKD | EPR distribution |
|  | Information reconciliation |
|  |  |
| Quantum Leader Election | (Uses Weak coin flipping) |
|  |  |
| Quantum Cheque | 1. Uses: QKD |
|  | 2. GHZ source |
|  | 3. Quantum memory |
|  | 4. Quantum 1-way function |
|  | 5. SWAP test |
| Quantum Coin | Clifford gates |
|  | Quantum memory |
| Quantum Token | BB84 Encoding and decoding |
|  | Quantum Memory |
| Wiesner Quantum Money | BB84 Encoding and decoding |
|  | Quantum Memory |
| Quantum Oblivious transfer | BB84 Encoding and decoding |
| Classical FHE for q circuits | TDO |
| Measurement-Only Universal Blind Quantum Computation | Graph state generation (C-Z, + states preparation, + quantum memory) |
|  | Equatorial plane measurements |
| Prepare-and-Send Quantum Fully Homomorphic Encryption | TDO |
| Prepare-and-Send Universal Blind Quantum Computation | Graph state generation (C-Z, + states preparation, + quantum memory) |
|  | Equatorial plane measurements |
| Certified Pseudo-Secret Random Qubit Generator (PSQRG) | BB84 Encoding Decoding |
|  | Quantum Memory |
| Prepare-and-Send Verifiable Universal Blind Quantum Computation | Graph state generation |
|  | Equatorial plane measurement |
|  | Quantum One Time Pad |
|  | Quantum memory (size depends on graph considered, do not need to store the whole graph) |
| Measurement-Only Verifiable Universal Blind Quantum Computation | Graph state generation (C-Z, + states preparation, + quantum memory) |
|  | Equatorial plane measurement |
|  | Quantum memory |
| Prepare-and-Send Verifiable Quantum Fully Homomorphic Encryption | TDO |
| Secure Multiparty Delegated Quantum Computation | Graph state generation |
|  | Verifiable secret sharing |
|  | TDO |
| State Teleportation | EPR state source and broadcasting |
|  | Bell measurements |
| Weak String Erasure | BB84 Encoding and Decoding |
| Certified Finite / Infinite Randomness Expansion | BB84 Encoding and Decoding |
|  | EPR generation between 2 measurement devices |

# Task extraction and categorisation

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Layer | TNetwork stage | Comment |
| 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 |  | Keep? |
| Teleportation protocol | Transport |  |  |
| Verification of stabilizer state | Off |  |  |
| (V)QSS | Off |  | Keep? |
| 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 |  |  |

# KG

# Software implementation recommendations

# Hardware integration recommendations