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, additional functionalities can be required 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. By doing so, we aim at providing building blocks that would:

* lessen the amount of code and control needed while developing applications for the quantum internet (in particular through code reuse);
* 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 quantum protocols.

# Methodology

1. Review of the quantum protocol zoo looking at the various protocols;
2. Identify and group 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) | BB84 encoding |
| <https://arxiv.org/abs/1403.5551> | BB84 decoding |
| Measurement Device Independent QDS | Classical authenticated channels |
| <https://arxiv.org/pdf/1704.07178.pdf> | Measurement Device Independent QKD link |
|  | BB8484 Encoding and Decoding |
| Multipartite Entanglement Verification | Authenticated classical channels |
| <https://www.nature.com/articles/ncomms13251> | Secure classical broadcast |
|  | Common shared randomness |
|  | Limited memory |
|  | BB84 Measurements |
|  | GHZ source / broadcast |
| Quantum Fingerprinting | Clifford gates |
| <https://arxiv.org/abs/quant-ph/0102001> | Swap test |
| BB84 | BB84 Encoding and Decoding |
| <https://core.ac.uk/download/pdf/82447194.pdf> | Authenticated classical channel |
|  | Privacy amplification |
|  | Information reconciliation |
| Device Independent QKD | EPR distribution |
| <https://arxiv.org/abs/1811.07983> | Information reconciliation |
|  |  |
| Quantum Leader Election | (Uses Weak coin flipping) |
| <https://arxiv.org/abs/0910.4952> |  |
| Quantum Cheque | (Uses QKD) |
| <https://link.springer.com/article/10.1007/s11128-016-1273-4> | GHZ source |
|  | Quantum memory |
|  | Quantum 1-way function |
|  | SWAP test |
| Quantum Coin | Clifford gates |
| <http://users.math.cas.cz/~gavinsky/papers/QuMoClaV.pdf> | Quantum memory |
| Quantum Token | BB84 Encoding and decoding |
|  | Quantum Memory |
| Wiesner Quantum Money | BB84 Encoding and decoding |
| <http://users.cms.caltech.edu/~vidick/teaching/120_qcrypto/wiesner.pdf> | Quantum Memory |
| Quantum Oblivious transfer | BB84 Encoding and decoding |
| <https://link.springer.com/chapter/10.1007/3-540-46766-1_29> |  |
| Classical FHE for Quantum Circuits | Full QC (server) |
| <https://arxiv.org/abs/1708.02130> |  |
| Measurement-Only Universal Blind Quantum Computation | Graph state generation (C-Z, + states preparation, + quantum memory) |
| <https://journals.aps.org/pra/abstract/10.1103/PhysRevA.87.050301> | Equatorial plane measurements |
| Prepare-and-Send Quantum Fully Homomorphic Encryption | Full QC (server) |
| <https://arxiv.org/abs/1603.09717> | Quantum OTP (client) |
| Prepare-and-Send Universal Blind Quantum Computation | Graph state generation (C-Z, + states preparation, + quantum memory) |
| <https://arxiv.org/abs/0807.4154> | Equatorial plane measurements |
| Pseudo-Secret Random Qubit Generator | Full QC on server's side |
| <https://arxiv.org/abs/1802.08759> | Quantum-safe one-way functions that are 2 regular, collision resistant (Client's side) |
| Prepare-and-Send Verifiable Universal Blind Quantum Computation | Graph state generation |
| <https://arxiv.org/abs/1203.5217> | 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) |
| <https://arxiv.org/abs/1208.1495> | Equatorial plane measurement |
|  | Quantum memory |
| Prepare-and-Send Verifiable Quantum Fully Homomorphic Encryption | Full QC (server) |
| <https://arxiv.org/abs/1708.09156> | Clifford QC (client) |
| Secure Multiparty Delegated Quantum Computation | Graph state generation |
| <https://arxiv.org/abs/1606.09200> | Verifiable secret sharing |
| State Teleportation | EPR state source and broadcasting |
|  | Bell measurements / CNOT Hadamard and computational basis measurements |
| Weak String Erasure | BB84 state preparation and measurement |
| Certified Finite / Infinite Randomness Expansion | CHSH Measurements |
|  | EPR generation between 2 measurement devices |

# Task extraction and categorisation

|  |  |  |  |
| --- | --- | --- | --- |
| Function | Layer | Network stage | Comment |
| Sending qubit | Transport | Trusted repeater | Should be provided by the Transport layer. |
| Sending qubit blocks | Transport | Trusted repeater | Should be provided by the Transport layer. |
| Teleportation protocol | Transport | Entanglement generation | Should be provided by the Transport layer. |
| Creation and braodcast of GHZ state | Session | Quantum memory | Core for GHZ relying protocols (directly tap into network layer) |
| Creation and broadcast of any stabilizer state | Session | Quantum memory | Core for GHZ relying protocols (directly tap into network layer) |
| Creation and broadcast of arbitrary graph states | Session | Quantum memory | Core for GHZ relying protocols (directly tap into network layer) |
| Quantum One Time Pad / confidential channel (encoding and decoding) | Presentation | Trusted repeater | Core |
| BB84 Encoding of classical data | Presentation | Trusted repeater | Core |
| BB84 Decoding to classical data | Presentation | Trusted repeater | Core |
| Single Qubit Preparation in equatorial plane (finite set of angles) | Presentation | Trusted repeater | Core |
| Single Qubit Measurement in equatorial plane (finite set of angles) | Presentation | Trusted repeater | Core |
| Multi qubit POVM | Presentation | Quantum memory | Assess usefulness / code repetition avoidance |
| Local Pauli gates | Off | - | Core |
| Local Clifford gates | Off | - | Core |
| Local memory | Off | - | Core |
| Non Clifford gates | Off | - | Core |
| Verification of stabilizer state | Off | - | Not atomic but useful to avoid code repetition |
| QFactory | Off | - | Core |
| Swap Test | Off | - | Core |
| Privacy amplification | Off | Classical | Core if throughput is important |
| Information reconciliation | Off | Classical | Core if throughput is important |
| Quantum 1 way function | Off | - | Not atomic but useful to avoid code repetition |
| Secure classical broadcast channel | Off | Classical | Core if protocol needs speed / low latency |
| Classical authenticated channel | Off | Classical | Core if protocol needs speed / low latency |
| Anonymous transmission channel | Session | Quantum memory | Not atomic but useful as building block |
| Quantum Authenticated Channel | Session | Quantum memory | Not atomic but useful as building block |
| Weak Coin Flipping | Application |  | Not atomic but useful as building block |
| (Verifiable) Quantum Secret Sharing | Application |  | Not atomic but useful as building block |