The Quantum Protocol Zoo

Shraddha Singh,[1] Mina Doosti,[2] Natansh Mathur,[1,3] Rhea Parekh,[1,4] Gözde Ustün,[1] Bas Dirkse,[5,6,7] Victoria Lipinska,[5,6] Jérémy Ribeiro,[5,6] Mahshid Delavar,[2] Niraj Kumar,[2] Gláucia Murta,[5,6] Atul Mantri,[2] Celine Chevalier,[8] Harold Ollivier,[1] Marc Kaplan,[9] and Elham Kashefi[1,2,*]

[1] *LIP6, CNRS, Sorbonne Université, France*
[2] *School of Informatics, University of Edinburgh, UK*
[3] *Department of Computer Science and Engineering, Indian Institute of Technology, Roorkee, India*
[4] *Department of Physics, Indian Institute of Technology, Roorkee, India*
[5] *QuTech, Delft University of Technology, Netherlands*
[6] *Kavli Institute of Nanoscience, Delft University of Technology, Netherlands*
[7] *QuSoft, CWI and University of Amsterdam, Netherlands*
[8] *CRED, Universite Pantheon-Assas, Paris II, France*
[9] *VeriQloud, France*

We introduce a framework for presenting the quantum communication protocols to make them readily realisable and applicable for a broad range of communities interested in the use cases of quantum technology. The framework describes the overall functionality of a set of protocols as well as presenting each protocol compactly and consistently. The practical realisation of this framework is - The Quantum Protocol Zoo - hosted at https://wiki.veriqloud.fr. As a preliminary work, several concrete protocols in this framework have been added to the protocol zoo. Furthermore, we develop a novel concept of resource visualisation for quantum communication protocols. This includes two user-friendly interfaces: *Protocol decomposition*, to identify the types of resources required for each protocol; and *Knowledge Graph*, an interactive interface connecting all the listed protocols with their required resources in a single graph. Although the existing protocols in the zoo have been chosen based on the expertise of present contributors, we intend to integrate many more families of the quantum network protocols soon. Using our framework, we aim to integrate all the quantum internet protocols to make the quantum protocol zoo a valuable resource towards realising real-world use-cases for the quantum internet, the development of applications, and future networks.

I. INTRODUCTION

Future information and communication networks will certainly consist of both classical and quantum devices, some of which are expected to be dishonest, with various degrees of functionality, ranging from simple routers to servers executing quantum algorithms. Most of the technology required to achieve advanced stages of a quantum internet [1] is still in its infancy, hence it is very hard to predict the potential use cases. Several applications, however, have already been characterized depending on the different stages of a quantum network [2]: secure delegated quantum computing [3–9], quantum key distribution [10–14], clock synchronization [15, 16], leader election [17], quantum digital signatures [18], quantum bit-commitment [19], quantum money [20] among others. Such applications promise to impact and transform the society on multiple levels including communication, accessing information and security. Therefore, it would be extremely useful to have a standard framework to describe the protocols that are relevant to quantum internet such that they apply to the diverse quantum information science community.

We take the first step in this direction and call such an initiative: *The Quantum Protocol Zoo* which consists of an organised collection of protocols that could be implemented (or simulated) over a quantum internet in the coming years. The idea behind quantum protocol zoo is inspired by the success stories and impact of the Complexity Zoo and the Quantum Algorithm Zoo, which are resourceful repositories to enrich and update our knowledge on complexity classes and quantum algorithms, respectively. In a similar spirit, the quantum protocol zoo is a wiki of quantum communication protocols for various functionalities classified in terms of the different network stages for quantum internet [1]. Although there are several different ways of formally defining a protocol, we characterise a protocol as a sequence of steps, specifically designed to accomplish a task, that either runs between trusted or dishonest multiple participants/nodes.

* For any questions and feedback: quantumprotocolzoo@gmail.com

The goal of this project is multifold. First, it aims to provide a compact and precise review of all the existing protocols in one place, such that it is accessible to both the young researchers motivated to enter into the field as well as "quantum enthusiasts" [1]. Second, our platform enables the experts from academia and industry to find real-life use cases for the listed protocols and at the same time innovate on (or compose) the existing ones to the tailor-made new protocol for the desired task. Third, we aim to develop a standardised framework for protocol descriptions to make the community "quantum-internet" ready. At the same time, we emphasise that our purpose is not to point out the strengths or weaknesses of any particular protocol or functionality.

With the rapid progress in quantum technologies and improvements in the existing protocols, it is extremely beneficial to have a resource visualisation for all the quantum protocols in one place that can be regularly updated to keep track of the advancements, something that can not be achieved with the review articles or a book. To this end, we introduce two user-friendly interfaces for resource visualisation. First, Protocol decomposition, where we classify the resources into multiple categories to decompose each protocol into these resource categories. Second, the Knowledge Graph, which is an interactive interface aimed at unifying the protocol decomposition. This is a comprehensive 'knowledge graph' which connects all the protocols with their resources in a single graph. We expect this would highly facilitate the protocol developers and experimentalists alike in finding links among different protocols and functionalities and the corresponding resource categories they can be decomposed into.

We, therefore, invite everyone from the quantum information science community to join and contribute to this initiative in collectively making the quantum protocol zoo a crucial source for quantum protocols.

II. ZOO FRAMEWORK

The final framework used for presenting protocols on the zoo is a result of fruitful discussions with quantum groups at TU Delft, LIP6 Sorbonne Université and School of Informatics at the University of Edinburgh. It has undergone several modifications after discussions with researchers and developers involved in classical internet security at ENS Paris, Security Groups at the University of Edinburgh, VeriQloud and SAP security group. Based on these discussions, two-page categories (functionality and protocol) have been defined for presenting the quantum protocols. We explain each of them in detail below.

A. Functionality page

For a family of related protocols implementing the same general task we define the functionality as their common root link in the zoo. Note that each protocol will implement the functionality in different ways discussed in the corresponding protocol page (see next section). Hence a functionality page gives only an overall picture of a class of quantum protocols including their main goal and the properties they need to provide. For example, the functionality page for the class of quantum digital signature schemes[2] describe the generation of the signed message as the main goal of any quantum digital signature scheme. The page also introduces the properties including *transferability*, *non-repudiation* and *unforgeability* which are necessary to provide for any quantum digital signature scheme. The functionality page consists of several sections that are represented in the following box.

- Functionality description: A lucid definition of functionality in the discussion.
- Tags: Related category pages or list of protocols are internally linked by this section.
- Use case: This section analyses how practical the protocol is, for industry use when compared to other alternatives. It answers the following questions:

[1] anyone who has basic knowledge of linear algebra and the postulates of quantum mechanics [21].
[2] https://wiki.veriqloud.fr/index.php?title=Quantum_Digital_Signature

  - Quantum or classical task?
  - Any classical or post-quantum secure analog?
  - Benchmark values for key length, a security parameter, threshold values, etc?
  - Scalability in terms of time, key length, etc.
  - Real World Applications?
- Protocols: List of different concrete protocols achieving the functionality (each protocol in this list is written in the format given in the protocol page box).
- Properties: All the properties that need to be satisfied by any protocol achieving the concerned functionality and other common terminologies used in all the protocols.
- Further information: Any issue that could not be addressed or find a place in the above sections or any review paper discussing a feature of various types of protocols related to the functionality.

B. Protocol page

Functionality pages contain the link to various protocols implementing them illustrated in the corresponding protocol page. Each protocol is defined by a sequence of steps precisely specifying the actions that need to be performed by two or more parties. The structure of the protocol page is shown in the following box.

- Protocol description: It differs from the generic root functionality description, highlighting how this specific protocol achieves the general task.
- Tags: Any related pages connected by this section.
- Assumptions: It describes the setting in which the protocol is running. Any assumption on the setup or limitation in the actions of parties is listed in this section.
- Outline: A non-mathematical detailed outline which provides a rough idea of the concerned protocol in a layman language.
- Notation: Consists of all the notations required for describing the protocol.
- Requirements: This section specifies the network stage[1] which the protocol belongs to, relevant network parameters as specified for each stage, hardware requirements for each party. Other available information from experimental implementations such as QBit error rate, no of qubits used, the order of digital threshold values, key length, a security parameter, scalability are also detailed in this section. It also consists of a diagram displaying the resource requirements of the protocol.
- Properties: A list of important information extracted from the protocol such as security claims related to the properties given in the root functionality.
- Protocol description: Functional step-wise protocol algorithm helpful to write the code for the simulation or actual implementation. Can be divided into stages common for all the protocols in the concerned functionality.
- Further information: Any useful information that could not find its place in the above description goes here. One could describe protocol steps with a simple example. Also, some pages on protocols might include a short description as below for a list of protocols in the same class of functionality and network stage that are easy to interpret after reading the concerned formal description (or are variants of the protocol discussed above).

- Theoretical papers:
  - How is it different from the above protocol
  - Requirements
  - Security
- Experimental papers:
  - Which paper or protocol does it implement
  - Benchmark values for this demonstration

III. ZOO MAP

The quantum protocol zoo also has a set of navigation tools to go around exploring different functionalities. The main page gives an exact format as that provided above and thence, directs the user to a few navigation tools on the sidebar. These tools have been configured for the quantum protocol zoo as follows:

- **Protocol library:** shows the list of functionalities covered in the protocol zoo along with their corresponding protocols.

- **Categories:** links various pages with common "Tags" which help the user to explore protocol zoo from a different perspective. As the zoo expands these categories are also changing. Currently, the items listed are two-party protocols; multi-party protocols; specific task; universal task; building blocks; network stage, etc.

- **Supplementary information**

  - Glossary: This tab explains notations used in various papers commonly used in quantum communication protocols.

  - Review papers: Various review papers on quantum communication and related topics have been enlisted here.

IV. RESOURCE VISUALISATION

Resource quantization is a necessary step for experimentalists aiming to achieve the realisation of protocols and also to demonstrate some form of advantage in using those resources. For example, for the quantum communication protocols such as quantum key distribution, the advantage would be demonstrating information-theoretic security in the key exchange, something that is elusive to traditional public-key cryptography schemes. Another scenario for the experimentalists would be, given the type and amount of resources they have, they would want to identify the range of protocols that can be implemented. In general, this is a time-consuming task and requires an in-depth knowledge of all the currently available protocols.

Furthermore, decomposing high-level functionalities to their sub-protocols and eventually their necessary resources construct a hierarchy based on which the building block protocols of a quantum network can be determined. Determining these building blocks can benefit both the experimentalists as well as to someone interested in designing protocols. For experimentalists, these protocols will be the first protocols that need to be implemented in their respective laboratories. For the theoreticians and protocol designers, on the other hand, this hierarchy will serve as an important toolkit for composing and constructing new protocols with more completed functionalities.

To bridge the gap between theory and practice, we propose two user-friendly solutions to the above-mentioned problem and implement them in the quantum protocol zoo. These are described in detail below.

A. Protocol decomposition

For each protocol in the zoo, we have identified the resources required by each participant. Moreover, we have classified the resources into multiple categories with separate notation for each category of resource.

- Physical resources: All the physical resources like communication channels (quantum or classical), state preparation, measurements, etc. come under this category. It mentions specific details wherever required, for example, non-separable multi-qubit state preparation, secure classical channel, quantum memory.
- Nodal subroutines: This refers to tasks to be performed at a single node and which do not require any communication. All the single party tasks like random number generation, classical processing, quantum one-time pad, among others come under this category.
- Other protocols and functionalities: Any other protocol and/or functionality which is required to be performed as a part of this protocol is mentioned in this category. For example, many protocols require quantum key distribution which comes under this category.

B. Knowledge Graph

For the unification and interactivity of the decomposition, we provide the all-encompassing Knowledge Graph, hosted at https://quantumprotocolzoo.github.io/posts/visualizations/, of the zoo which is a graph connecting all the protocols and their required resources in one single graph. This knowledge graph serves a dual purpose in its role of easing the interaction between theorists and experimentalists.

- By selecting any specific functionality, it highlights all the protocols in the zoo which perform it along with the resources required by each of them. The same can be achieved by selecting any specific protocol. The graph will highlight the resources for performing the protocol.
- By selecting the resources at disposal to an experimentalist, the graph highlights the protocols and functionalities which can be implemented using them. This serves as an excellent initial resource for those who wish to implement protocols or wish to perform benchmarking for identifying which protocols they can perform without having to go through all the research papers.

V. HOW TO CONTRIBUTE TO THE ZOO?

The quantum protocol zoo has been started as an attempt to build a comprehensive record of different quantum protocols ranging from fundmental protocols such as quantum cloning, quantum teleportation and quantum entanglement distribution; simple cryptographic protocols such as quantum key distribution, digital signature, coin flipping, quantum money; all the way to more composite quantum computing protocols such as secure delegated quantum computation and secure multiparty quantum computation. It is a dynamic platform to incorporate with the primary purpose to easily update new results in the future. Being an open platform, all the researchers and practitioners who work on designing and implementing quantum protocols are invited to access or expand the zoo with further contributions. Anyone can add a new protocol to the zoo or complete the existing ones with other reference data, experimental data, use cases and/or security analysis. Since the platform presents a brief overview of each protocol while covering its full detail, all the people from academia and industry including physicist, mathematicians, cryptographers, computer scientists, electrical engineers, software developers and so on can get their required information with much less effort than reading several full papers. In this way, the contributors will get benefits of further dissemination of their works among a broader range of audiences while their contributions will be also cited under their name at the further information section in the corresponding page.

Submission guideline. A detailed guideline on submission format is provided in the "How to submit" section of the main page[3]. Any comment or query related to submissions, content or structure of the zoo

[3] https://wiki.veriqloud.fr/index.php?title=Main_Page

pages can be addressed at quantumprotocolzoo@gmail.com. In case of minor comments, one can also use the "Discussion" tab at the top of each page in the quantum protocol zoo.

It is worth mentioning that the contributors do not need to fully complete all the sections introduced in the guidelines since some of the protocols may not be studied or experimentally implemented as much as the other protocols such as QKD and Quantum Digital Signatures. So, for example, the hardware requirement may not be provided for some of the protocols.

VI. FUTURE WORK

The current format of quantum protocol zoo will be further expanded and developed across multiple different directions. One of the primary goals would be to have a deeper analysis of the existing protocols in the zoo as well as enriching it with new protocols and functionalities. This would also help in achieving a standardisation for all the possible functionalities that can be implemented on a quantum network. We are currently developing an open-source library of the codes for the protocols in the zoo, inspired by the modular programming techniques, which would facilitate the simulations of the quantum protocols on the quantum internet software such as SimulaQron[4] [22] available at our Quantum Protocol Zoo's Repository[5]. The link to the new code would be also added to the relevant pages on the protocol zoo.

We intend to use the framework of Abstract Cryptography (AC) [23] to define an ideal resource for each protocol that would be described in terms of its subroutines. The AC terminology would eliminate any unnecessary information from the protocol, thereby making it understandable for a wider group of readers. Similarly, using a standard language would help both the cryptography community to explore security proofs and experimentalists to explore a modular implementation of protocols.

We would also like to expand further our hardware requirement analysis for each protocol in the protocol zoo. This would help to characterise the protocols into different quantum internet stages with concrete benchmarking values.

VII. ACKNOWLEDGEMENTS

The authors acknowledge financial support from the ANR International Project VanQute; the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 820445 (QIA); The UK Engineering and Physical Sciences Research Council Grant No. EP/N003829/1 as well as technical supports from VeriQloud for hosting the Zoo and all members of Paris Center for Quantum Computing for their generous time in endless many discussions for setting up the zoo.

[1] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[2] Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. Quantum internet: from communication to distributed computing! *arXiv preprint arXiv:1805.04360*, 2018.

[3] Andrew M Childs. Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466, 2005.

[4] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[5] Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. Interactive proofs for quantum computations. *arXiv preprint arXiv:1704.04487*, 2017.

[6] Tomoyuki Morimae and Keisuke Fujii. Blind quantum computation protocol in which alice only makes measurements. *Physical Review A*, 87(5):050301, 2013.

[7] Anne Broadbent. Delegating private quantum computations. *Canadian Journal of Physics*, 93(9):941–946, 2015.

[4] http://www.simulaqron.org/

[5] https://quantumprotocolzoo.github.io/

[8] Joseph F Fitzsimons. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1):23, 2017.
[9] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of computing systems*, pages 1–94, 2018.
[10] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.
[11] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11, 2014.
[12] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.
[13] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.
[14] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2:16025, 2016.
[15] Richard Jozsa, Daniel S Abrams, Jonathan P Dowling, and Colin P Williams. Quantum clock synchronization based on shared prior entanglement. *Physical Review Letters*, 85(9):2010, 2000.
[16] Isaac L Chuang. Quantum algorithm for distributed clock synchronization. *Physical review letters*, 85(9):2006, 2000.
[17] Vasil S Denchev and Gopal Pandurangan. Distributed quantum computing: A new frontier in distributed systems or science fiction? *ACM SIGACT News*, 39(3):77–95, 2008.
[18] Daniel Gottesman and Isaac Chuang. Quantum digital signatures. *arXiv preprint quant-ph/0105032*, 2001.
[19] Gilles Brassard and Claude Crépeau. Quantum bit commitment and coin tossing protocols. In *Conference on the Theory and Application of Cryptography*, pages 49–61. Springer, 1990.
[20] Charles H Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology*, pages 267–275. Springer, 1983.
[21] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.
[22] Axel Dahlberg and Stephanie Wehner. Simulaqron—a simulator for developing quantum internet software. *Quantum Science and Technology*, 4(1):015001, 2018.
[23] Ueli Maurer and Renato Renner. Abstract cryptography. In *In Innovations in Computer Science*, 2011.