

SimulaQron - A simulator for developing quantum internet software

Axel Dahlberg¹ and Stephanie Wehner¹

¹*QuTech, Lorentzweg 1, 2628 CJ Delft, Netherlands*

We introduce a simulator for a quantum internet with the specific goal to support software development. A quantum internet consists of local quantum processors, which are interconnected by quantum communication channels that enable the transmission of qubits between the different processors. While many simulators exist for local quantum processors, there is presently no simulator for a quantum internet tailored towards software development. Quantum internet protocols require both classical as well as quantum information to be exchanged between the network nodes, next to the execution of gates and measurements on a local quantum processor. This requires quantum internet software to integrate classical communication programming practises with novel quantum ones.

SimulaQron is built to enable application development and explore software engineering practises for a quantum internet. SimulaQron can be run on one or more classical computers to simulate local quantum processors, which are transparently connected in the background to enable the transmission of qubits or the generation of entanglement between remote processors. Application software can access the simulated local quantum processors to execute local quantum instructions and measurements, but also to transmit qubits to remote nodes in the network. SimulaQron features a modular design that performs a distributed simulation based on any existing simulation of a quantum computer capable of integrating with Python. Programming libraries for Python and C are provided to facilitate application development.

PACS numbers:

I. INTRODUCTION

A quantum internet enables quantum communication between remote quantum processors in order to solve problems that are infeasible classically. Many applications of a quantum internet are already known, the most famous of which is quantum key distribution (QKD) [1, 2] which allows two network nodes to establish an encryption key. Examples of other applications are secure identification [3] and other two-party cryptographic tasks [4], clock synchronization [5], secure delegated quantum computation [6], and even extending the baseline of telescopes [7]. For many of these applications, only relatively simple quantum processors capable of operating on a handful of qubits are required, as they draw their power from quantum entanglement. Entanglement can be realized using already one qubit at each end point, and its capabilities cannot be replicated using classical communication. In the case of QKD, for example, quantum processors capable only of preparing and measuring single qubits can already be sufficient [1].

The first quantum networks that connect remote quantum processors capable of operating on several qubits each are expected to be deployed within the coming years. In order to execute arbitrary quantum internet applications on these networks, it is essential to create a development framework in which software for these applications can be written and debugged. Writing software for a quantum internet shares some similarities with programming a quantum computer, but in addition poses new challenges. Similar to programming a quantum computer, we wish to execute quantum gates and measurements on each local quantum processor. Techniques for optimizing

such gates and mapping them to the underlying hardware can be borrowed from quantum computing efforts, and are hence not the subject of this work. What differentiates programming a quantum network is the need for a close integration between classical and quantum messages exchanged during the course of the protocol. The need for such integration arises at several layers of abstraction, and poses significant design challenges. On a lower level, a quantum network stack is needed to create and track entanglement in the network, which requires classical control messages to be exchanged. On a higher level, applications which desire to create and use such entanglement do themselves exchange classical messages during the course of a protocol, requiring standard classical network programming techniques to integrate with quantum ones. At present, a full quantum network stack is missing, and no software development framework for writing quantum network applications exists.

A. What SimulaQron does

SimulaQron is a simulator written precisely to provide an essential tool for software development for a quantum internet. Specifically, SimulaQron simulates several quantum processors, connected by a simulated quantum communication channels. Each simulated processor may thereby run on a different classical computer, and supports the execution of local quantum gates and measurements, as well as commands for sending qubits to remote nodes. A schematic picture of the communication between the nodes in a network simulated by SimulaQron is given in Figure 1. SimulaQron transparently simulates

the exchange of qubits and the creation of entanglement between remote processors in the background, making this functionality available to applications. To perform the simulation of local quantum processors itself, SimulaQron’s modular structure does in principle allow any simulation of a quantum computer accessible via Python to serve as a backend. The key novelty in SimulaQron is to use such backends as the basis for a distributed simulation that maps locally simulated entangled qubits to remote network nodes, in order to simulate the availability of entanglement between distant computers. We emphasize that applications using SimulaQron’s simulated entanglement, evidently do not provide the security guarantees afforded by real entanglement. The objective is instead to use SimulaQron as a development platform to write software realizing these applications which can later run on real quantum hardware and use real entanglement in order to achieve these guarantees. SimulaQron can be used as a tool for software development in all areas ranging from the implementation of the actual applications, the development of application level abstractions and programming libraries, to implementing a quantum network stack.

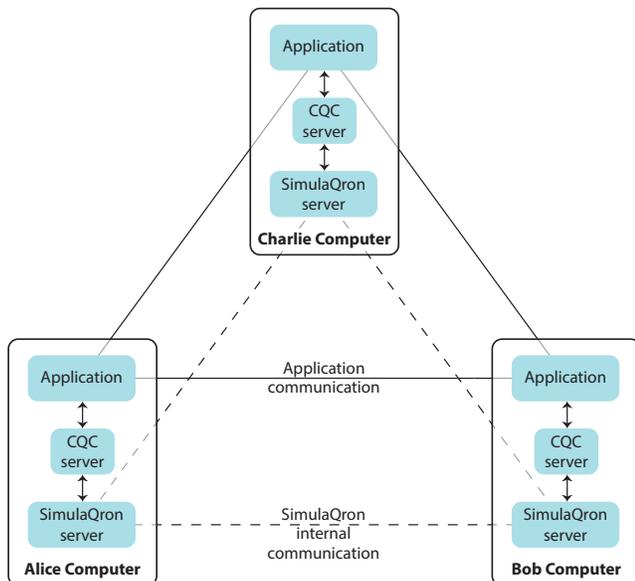


FIG. 1: A schematic overview of the communication in a quantum network simulated by SimulaQron. The simulation of the quantum hardware at each node is handled by the SimulaQron server. Communication between the SimulaQron servers is needed to simulate the network, for example to simulate entanglement. Opting for this method enables a distributed simulation, i.e. the computers in the figure can be physically different computers. The CQC servers provide the CQC interface to the applications running on the network and the simulated hardware (see also Figure 2). Finally the applications can communicate classically, as they would do in a real implementation of a quantum network.

B. What SimulaQron does not

We emphasize that SimulaQron is written as a tool for software engineers, with the objective of allowing software engineering efforts for a quantum internet to proceed. Its goal is thus to allow developers to write software that can later run with no or minimal modification on real quantum internet hardware. SimulaQron, however, does not aim to achieve an efficient simulation of a large scale quantum internet in order to test quantum repeater schemes, error correcting codes, or study the effects of noise on distant qubits. Such low level simulation capabilities which are of interest to quantum information protocol designers are the subject of a separate simulation platform (NetSquid [8]), which performs a discrete event simulation of a large scale quantum internet capable of modelling timing delays and hence study the effects of delays in quantum, as well as classical control communication on the performance of quantum protocols and a quantum network stack.

For software engineers, we remark that there are some things which are purposefully not handled by SimulaQron. This includes, for example, the management and tracking of entanglement required by a quantum network stack, which may be explored and implemented using SimulaQron. Importantly, we also note that for the same reason no efforts have been made to secure or authenticate access to the simulated quantum processors. A SimulaQron backend server will by default happily accept requests from any client connecting to it, and in particular allow access to any qubit given its correct identifiers. It is clear that mechanism for implementing access control to quantum nodes and qubits is important to realize in software for a quantum internet, highlighting the need for a tool like SimulaQron as a stand-in for quantum hardware in order to develop them.

C. Related Work

There is to our knowledge no analogue of SimulaQron available for application development on a quantum internet. There are of course numerous simulators of a quantum computer available, some of which could in principle be used as a local simulation backend in conjunction with SimulaQron. Freely available ones include ProjectQ [9] which uses Python, and also contains an optimizing compiler. Other simulators include Liquid [10] (available as a binary), and QX [11]. Presently, the quantum backend of SimulaQron is simply realized using QuTip [12], which is not designed to be an efficient simulator, but more than sufficient for the purpose of simulating a small network. Using QuTip has also the advantage to provide a very easy way to extend SimulaQron to operate on noisy instead of perfect qubit, should one wish to gain insights into whether, for example, code performing error correction for a quantum protocol has been implemented correctly.

D. Overview

SimulaQron itself is written in Python [13] due to the popularity of this language in the quantum information community, making it easier to extend if desired. Internally, SimulaQron also makes use of the Twisted framework for Python [14]. SimulaQron’s simulated quantum internet can be programmed in two ways as outlined in Figure 2. In Section II we will provide an overview of the design and inner workings of SimulaQron. In Section III we discuss the integration with the CQC interface. We provide two simple examples on how to program SimulaQron using the Python CQC library in Section IV. Further examples, programming templates as well as an API documentation can be found online [15]. Finally, we discuss future developments and extensions of SimulaQron.

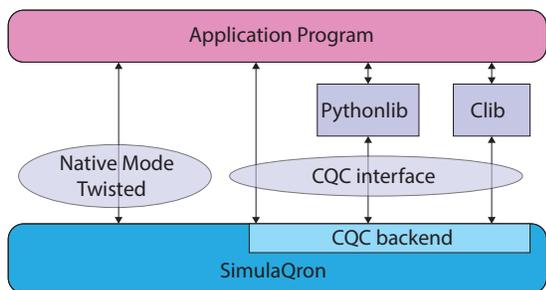


FIG. 2: SimulaQron’s simulated quantum internet can be programmed in two ways. The first proceeds by directly accessing the SimulaQron backend using Twisted in Python. This way of programming gives full access to the backend, but is highly specific to Twisted and unlikely to be available on any real quantum network devices of the future. The second way of programming SimulaQron is by using its Classical-Quantum-Combiner (CQC) interface. CQC specifies a packet format for issuing commands to a quantum network node and we intend to make a (possibly refined) version of CQC available on the planned 2020 quantum internet demonstrator in the Netherlands using actual quantum network hardware. For ease of programming, we provide two libraries that encapsulate the CQC interface. More specifically, we provide libraries in both Python and C for programming quantum internet applications, which internally connect to SimulaQron over the CQC interface. Libraries for other languages are easy to add and can access SimulaQron using the CQC interface.

II. BACKEND

Let us now first describe the SimulaQron backend, which can be accessed in Python using Twisted’s Perspective Broker [14]. We note that for programming applications there is no need to ever access the backend directly, as the Python library using CQC provides a much easier way to program applications. CQC furthermore provides an interface (close to) what we intend to make available on the quantum internet demonstrator in the

Netherlands that can be accessed from any programming language.

The main challenge in providing a simulator suitable for programming quantum internet applications is to simulate quantum entanglement. Mathematically, any quantum state can be written as a density matrix $\rho \in \mathbb{C}^{d \times d}$, where d is the dimension of the quantum system (see [16], or [17, Weeks 0 and 1] for an introduction to quantum information). Crucially, for two entangled qubits A and B , we have $\rho \neq \sum_j p_j \rho_j^A \otimes \rho_j^B$, with $\rho_j^A \in \mathbb{C}^{d_A \times d_A}$, $\rho_j^B \in \mathbb{C}^{d_B \times d_B}$, and \otimes denoting the tensor product. This means that we cannot factorize ρ into different components ρ_j^A and ρ_j^B that could be simulated individually on two different network nodes. Instead, we need to simulate the entire matrix ρ as one, while making qubits A and B virtually available at two different nodes in the network.

This consideration motivates the design of the SimulaQron backend depicted in figure 3. The SimulaQron backend consists of a running a client and server program on each classical computer - a `virtualNode` - that wants to participate in the simulated quantum network. All such programs connect to each other, forming the simulated quantum internet backend.

SimulaQron itself does not provide a new quantum simulator, but rather builds a distributed simulation on top of an existing one using a modular design. In the initial release, we have simply used QuTip for the underlying simulation, but essentially any existing simulator (or even real quantum computing - but not yet networked - hardware) that can be addressed via Python can easily be used in conjunction with SimulaQron. An existing simulator can be made available to SimulaQron as a backend by providing an interface in the form of a `quantumEngine` to function as a `quantumRegister`. This register supports addressing individual qubits by their position in the register, that is, for an n -qubit register. For example, if say a Hadamard gate H is requested on the j -qubit, `quantumRegister` is responsible for applying this operation on the underlying quantum simulation. In the simple case of QuTip, this means simply applying the unitary $\text{id}^{\otimes j-1} \otimes H \otimes \text{id}^{\otimes n-j}$ to the matrix representing ρ (see `crudeSimulator.py`).

Building on top of an underlying `quantumRegister`, SimulaQron uses a `simulatedQubit` object to represent each qubit simulated in the underlying `quantumRegister`. Manipulation of qubits then follows exclusively by manipulating such `simulatedQubit`s without interacting directly with `quantumRegister`. In particular, each `simulatedQubit` keeps track of its own position in the register, allowing an easy manipulation and update of qubits that are physically simulated at a particular node. Specifically, for example, if a qubit is measured it can be removed from the underlying `quantumRegister` effectively shrinking the size of the matrices. This allows the simulation to proceed without

the underlying register to grow arbitrarily while new qubits are being created and discarded. Removal from the `quantumRegister` can be done while updating only the simulated qubits (and not anything manipulating them), and hence the rest of the simulation can proceed to access the simulated qubits without being aware the underlying register has been shrunk. Figure 3 illustrates the relationship between the `quantumRegister` and the `simulatedQubit`s. We note that `simulatedQubit` objects are local to the node performing their actual simulation in the `quantumRegister`.

A. Virtual Qubits

Each `simulatedQubit` object is then associated with a `virtualQubit` object. Importantly, a `virtualQubit` does not need to reside at the same network node as the corresponding `simulatedQubit`, but can be transferred to other nodes than the one performing the backend simulation. Specifically, each `virtualNode` can hold a number of `virtualQubits` which can either be simulated locally (i.e., the simulated qubit the virtual qubit represents is located at the same node), or at a remote node. Twisted’s Perspective Broker is used to marshal the mapping of virtual qubits back to simulated qubit objects at remote nodes on the simulated network.

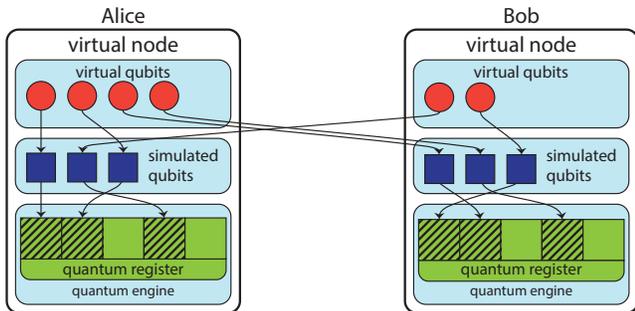


FIG. 3: A visualization of the interplay between different internal components of SimulaQron. The `simulatedQubit`s (blue squares) are objects handled locally in a `virtualNode`. These `simulatedQubit`s point to a part of the `quantumRegister`, which stores the state simulated by the `virtualNode`. Operations on the simulated state in the `quantumRegister` are handled by the `quantumEngine`. Additionally, a `virtualNode` also have `virtualQubit`s (red circles). These `virtualQubit`s point to `simulatedQubit`s, possibly in a different `virtualNode`. The `virtualQubit`s correspond to the actual qubits a node would have in a physical implementation of the quantum network.

This way it is possible for SimulaQron to simulate entanglement between network nodes: If simulated nodes A and B hold entanglement, then each `virtualNode`

has a `virtualQubit` that can be processed at nodes A and B as if they were truly entangled. In the background, however, the two virtual qubits are mapped back to two `simulatedQubit`s within the same `quantumRegister` that may be located at either A or B , or even some other node.

Any application wishing to use SimulaQron consists of a client program at each computer that connects to the SimulaQron server backend. SimulaQron will make virtual qubits available to any client connecting to the `virtualNode` server, as well as allow the creation of new qubits and registers. Using Twisted’s Perspective Broker, the client has full access to the specific virtual qubit, allowing it to perform gates, measurements, or send the qubit to other nodes in the simulated quantum network.

B. Register merges

One simple way to deal with virtual qubits is to have them simulated at one single classical computer in the network. Evidently, this puts a large strain on that specific computer, which then has to simulate every single qubit in the network. Here, we have chosen instead a distributed simulation, which is more challenging to realize, but does allow many nodes to take part, as long as the global entanglement in each quantum state is not too large. This is typically the case, when investigating how to program applications that may each run on only a subset of the nodes in the network.

We hence allow any `virtualNode` to hold a `quantumRegister` containing simulated qubits that may eventually be sent as virtual qubits to other nodes in the network. This enables a distributed simulation in which each classical computer participating in the simulated quantum internet contributes its share to realizing the overall simulation. Yet, it is clear that this approach brings additional challenges. Specifically, consider two virtual qubits A and B at one or more network nodes, which are mapped back to two simulated qubits in *different* `quantumRegister`s. An example of such a situation is given in Figure 4. If the protocol now requests the `virtualNode` to perform an entangling gate between A and B , qubits A and B may now become entangled and can thus no longer be simulated in different registers.

Entangling gates may thus require a register merge in order for the simulation to proceed. More precisely, entangling A and B then requires that the two distinct quantum registers which hold the corresponding simulated qubits are merged into one single quantum register, followed by an update of the corresponding `simulatedQubit`s that the `virtualQubit`s are mapped to.

SimulaQron solves this problem by transparently merging the registers in the background. For the application dealing with only the `virtualQubit`s such a merge is invisible, but the simulated qubits representing the virtual qubits in question are updated.

It is clear that locking is required to ensure consistency in performing such register merges in case multiple requests to merge a register arise in the network at the same time. At present, SimulaQron implements a very simple and relatively inefficient locking mechanism tailored to acquiring the minimal set of locks required to perform and update. As two separate locks for registers and simulated qubits are used, a deadlock can arise which is dealt with using a simple randomized backoff to marshall competition for locks. Future versions of SimulaQron may be enhanced by a more sophisticated locking mechanism.

III. CQC

On top of the backend, SimulaQron realizes a CQC interface (classical-quantum combiner) as implemented by the so-called CQC backend. CQC is a simple format in which SimulaQron can be programmed using any language capable of connecting to the CQC server backend over a TCP connection, and sending packets of the required form. In essence, the CQC instruction format provides a low level language programmable at the level of quantum gates and measurements, tailored specifically to include certain commands and behaviour that is useful in the quantum internet domain.

Two libraries are included to program SimulaQron via the CQC interface in Python and C. Programming SimulaQron via this Python library is the easiest way to make use of SimulaQron and the recommended way to get started using SimulaQron. Below, we provide two simple examples; many more examples can be found in the online documentation [15].

We expect that the present CQC interface will undergo further evolution until its use in the Dutch demonstration network. As such, we describe the main ideas and what functionality exists. The current version of the CQC interface including the precise message format is available online [15] and will be updated when a newer version exist. CQC specifies a particular instruction format for requests and replies from the CQC backend. Requests may be given as a single message to the CQC interface, or an entire batch of messages at once specifying a complex operation consisting of many actions in succession.

Messages in the CQC interface can be of different *types*, as described in section III A. One of these types is `COMMAND` which instructs SimulaQron (or the physical hardware) to perform a certain command. This command could for example be a gate or to send a qubit to another node. More details on the message type `COMMAND` is given in section III B.

In addition to the type of message and what command to perform, CQC messages will also contain information regarding for example the CQC version, an application identifier, the length of the message (including additional commands if any) and - if applicable - the qubit identifiers a command concerns, the IP and port-number the node a qubit should be sent to. Other options that can be

specified is whether notification should be returned when the command is finished and if the node should be blocked during the execution of the command, see table I.

Option	Effect
<code>OPT_NOTIFY</code>	Send a notify when command is done
<code>OPT_ACTION</code>	Execute further commands when done
<code>OPT_IFTHEN</code>	Execute further commands based on result
<code>OPT_BLOCK</code>	Block until cmd done

TABLE I: Options that can be specified when sending a `COMMAND` message.

There is also the possibility to attach a list of commands that should be executed directly after the command specified in the CQC message is completed, or if, for example, a measurement outcome takes on a certain value. As such, it is assumed that the CQC backend provides a rudimentary form of classical logic next to the quantum specific instructions that allow certain simple processing to be executed in the CQC backend, or indeed the actual hardware. That is, these commands can be executed without having to send messages back and fourth through the CQC interface between each command. Avoiding these messages between each command allows the sequence of commands to be executed faster, which is important for a physically implemented quantum network, subject to decoherence.

A. Message types

We describe in this section message types currently implemented in the CQC interface. As mentioned above, in future version of the interface, changes may be made and the latest version can be found online. The type that concern messages sent from the application to the hardware (either simulated by SimulaQron or physically implemented) are specified in table II.

Type	Effect
<code>TP_HELLO</code>	Alive check
<code>TP_COMMAND</code>	Execute (list of) command
<code>TP_FACTORY</code>	Execute (list of) command repeatedly
<code>TP_GET_TIME</code>	Get creation time of qubit

TABLE II: Types of messages from the application to the hardware/SimulaQron.

What commands can be specified using the type `COMMAND` is discussed in the following section. `FACTORY` is a type used similarly as `COMMAND`, but here a certain command should be executed a specified number of times. As an example of the use of `FACTORY` is to instruct the hardware to continuously produce a specified number of entangled EPR-pairs. An EPR-pair is then ready to be

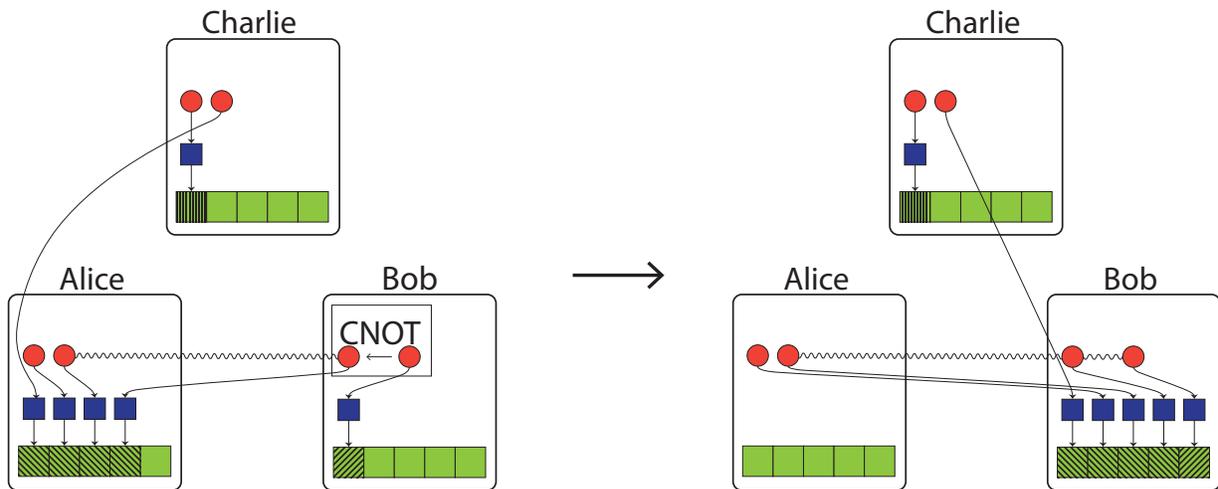


FIG. 4: A visualization of a register merge, initialized by a CNOT performed in the `virtualNode` Bob. Alice and Bob initially share a EPR-pair, represented by a curvy line between the two `virtualQubit`s. These entangled qubits are simulated in the `virtualNode` Alice. Bob then performs a CNOT between his part of the entangled state (target) and another qubit (control) simulated at Bob. This operations requires a register merge between Alice and Bob, since the three relevant qubits will now be in a GHZ-state, which needs to be simulated locally. The registers of Alice and Bob are therefore merged and all qubits simulated by either Alice or Bob are now simulated by Bob. Note that this also includes the `virtualQubit` of Charlie, which is initially simulated by Alice.

used whenever it is needed by the protocol running on the network.

There are also be message types returned by the hardware to the application, as specified in table III.

Type	Effect
TP_NEW_OK	Qubit was created
TP_EXPIRE	Qubit has expired
TP_DONE	Done with command
TP_RECV	Received qubit
TP_EPR_OK	Created EPR pair
TP_MEASOUT	Measurement outcome
TP_INF_TIME	Return timing information
ERR_GENERAL	General purpose error
ERR_NOQUBIT	No more qubit (or unknown qID)
ERR_UNSUPP	Sequence not supported
ERR_TIMEOUT	Timeout

TABLE III: Types of messages from the hardware/SimulaQron to the application.

B. Possible commands

The different commands currently supported in the CQC interface when using the message type `COMMAND` are specified in table IV. The full CQC packet format includes qubit and entanglement identifiers required by the commands below [15].

The angle of rotation for the single-qubit rotations are currently specified by one byte and is therefore discretized to 256 possible angles. When the creation of an EPR pair is requested, a message containing an entanglement identifier will be returned to the application. At present, there is no protocol to track and manage entanglement in a network available. We are currently developing and testing such a protocol, which will be referenced on the SimulaQron website once released [15].

IV. EXAMPLES

We provide here a simple example of how to program SimulaQron using the Python CQC library. More examples, also using the C CQC library, can be found in the full online documentation [15]. Before running the example presented here, the simulated network we consider needs to be configured and the servers that does the communication in the backend of SimulaQron has to be setup. Information on how to configure the simulated network and setup the servers can be found in the online documentation [15]. In what follows, we will hence assume that the SimulaQron and CQC backends have been setup already, simulating the hardware of two quantum internet nodes labelled Alice and Bob. We remark that the names Alice and Bob are translated by the Python CQC library into IP addresses according the configuration file specified on [15].

Command	Effect
CMD_I	Identity
CMD_NEW	Ask for a new qubit
CMD_MEASURE	Measure qubit (demolition)
CMD_MEASURE_INPLACE	Measure qubit (non-demolition)
CMD_RESET	Reset qubit to $ 0\rangle$
CMD_SEND	Send qubit to another node
CMD_RECV	Ask to receive qubit
CMD_RECV_EPR	Ask to receive half of EPR pair
CMD_EPR	Create EPR pair with another node
CMD_SWAP	Entanglement swapping
CMD_X	Pauli X
CMD_Y	Pauli Y
CMD_Z	Pauli Z
CMD_H	Hadamard
CMD_K	K gate (Z to Y)
CMD_T	T gate
CMD_ROT_X	Rotation around X (multiple of $\frac{2\pi}{256}$)
CMD_ROT_Y	Rotation around Y (multiple of $\frac{2\pi}{256}$)
CMD_ROT_Z	Rotation around Z (multiple of $\frac{2\pi}{256}$)
CMD_CNOT	CNOT (this as control)
CMD_CPHASE	CPHASE (this as control)

TABLE IV: Commands that can be specified when using the type `COMMAND`.

A. Sending BB84 States

The first example we consider has no classical communication on the application level between Alice and Bob. This implies that we do not need to set up a separate client/server interaction to exchange information at the level of applications. This means that Alice and Bob only connect locally to the CQC backend of SimulaQron, which functions as the quantum hardware at their network node, to issue quantum instructions. In this example, Alice will send a single qubit to Bob.

1. Code for Alice

The first thing we need to do is to initialize an object called a `CQCConnection`, which does the communication with SimulaQron using the CQC interface. Once this connection is set up, Alice has access to her own locally simulated quantum hardware.

```
from SimulaQron.cqc.pythonLib.cqc import *

# Establish connection to SimulaQron
Alice=CQCConnection("Alice")
```

The argument that `CQCConnection` takes should be the name specified in the configuration file for the

CQC-network. Once the connection is set up we can then create our first qubit. The `qubit`-object takes a `CQCConnection` as argument when initialized. When operations are applied to the `qubit`, the `CQCConnection` is used to communicate with SimulaQron, such that the corresponding simulatedQubit is updated.

```
# Create new qubit
q=qubit(Alice)
```

Alice will then send Bob one out of the four states

$$|0\rangle, |1\rangle, |+\rangle, |-\rangle \quad (1)$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, depending on the choice of the bits h_A and x set in the program. The states in equation 1 are usually called BB84-states and can be described by two binary variables as follows

$$H^{h_A} X^x |0\rangle \quad h_A, x \in \{0, 1\}, \quad (2)$$

where H is the Hadamard operation and X is the Pauli-X operation, defined as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (3)$$

The second part of the code on Alice side will then apply the operation $H^{h_A} X^x$, send the qubit to Bob. In our simple example, Alice is done using the quantum internet and hence we close the `CQCConnection`.

```
# Determine which BB84 state to use
h_A=1;x=0

# if x=1, flip |0> to |1>
if x == 1: q.X()

# if h_A==1, convert to Hadamard basis
if h_A==1: q.H()

# Send qubit to Bob
Alice.sendQubit(q, "Bob")

# Close connection to SimulaQron
Alice.close()
```

2. Code for Bob

We will now describe the code on Bobs side. In our example, Bob does nothing but wait for a qubit to arrive. Once he receives one, he will measure it in the standard- ($\{|0\rangle, |1\rangle\}$) (for $h_B = 0$) or the Hadamard-basis ($\{|+\rangle, |-\rangle\}$) (for $h_B = 1$) and print the measurement outcome. The code on Bobs side can be seen below, where `h_B` determines that basis Bob measures in.

```
from SimulaQron.cqc.pythonLib.cqc import *

# Establish a connection to SimulaQron
```

```

Bob=CQCCConnection("Bob")

# Choose which basis we measure in
h_B=1

# Wait to receive a qubit
q=Bob.recvQubit()

# If we chose the Hadamard basis
# to measure in, apply H
if h_B==1: q.H()

# Measure the qubit in the standard
# basis and store the outcome in m
m=q.measure()

# Print measurement outcome
print("Bobs meas. outcome: {}".format(m))

# Close connection to SimulaQron
Bob.close()

```

Note that if $h_A = h_B$ the measurement outcome for Bob will be Alice's choice of x with probability one.

B. Teleporting a qubit

In our second example, Alice teleports a qubit to Bob. This example demonstrates how to create shared EPR pairs, and also how to perform additional classical communication from Alice and Bob on the application level. This classical communication can be realized using standard client/servers programming. An inefficient, but convenient testing tool, to perform classical communication tool is provided by the Python library (see example 2) that does not require knowledge of classical client/server programming.

1. Code for Alice

As in the previous example, the first thing that happens is that a `CQCCConnection` is initialized to handle the communication to SimulaQron via the CQC interface.

```

# Initialize the connection
Alice=CQCCConnection("Alice")

```

By calling the method `createEPR`, Alice makes a request to generate an EPR-pair with Bob, i.e. to generate the state $\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$.

```

# Make an EPR pair with Bob
qA=Alice.createEPR("Bob")

```

When the EPR-pair has been generated, Alice prepares another qubit `q` in the state $|+\rangle = H|0\rangle$, which she wants to teleport to Bob.

```

# Create a qubit to teleport
q=qubit(Alice)

# Prepare the qubit to teleport in |+>
q.H()

```

Alice makes a Bell-measurement between the qubit `qA` in the EPR-pair shared with Bob and the qubit `q`. The Bell-measurement is done by applying a CNOT gate with `q` as control and `qA` as target, followed by a Hadamard gate on `q` and measuring both qubits in the standard basis.

```

# Apply the local teleportation operations
q.cnot(qA)
q.H()

# Measure the qubits
a=q.measure()
b=qA.measure()
print("Alice meas. out.: a={}, b{}".format(a,b))

```

At this point Alice needs to communicate to Bob what her measurement outcomes was, such that Bob can recover the state which is teleported. This classical communication can be realized by setting up a client/server interaction between Alice and Bob. There is a built-in feature in the Python library that realize this functionality, which have been developed for ease of use for someone not familiar with a client/server setup. This communication is also handled by the object `CQCCConnection`. For Alice to be able to send a message to Bob, Bob needs to first start a server by running `Bob.startClassicalServer()`. Alice will then apply the method `Alice.sendClassical("Bob",msg)`, where `msg` is the message she wish to send to Bob. The method checks if a socket connection is already opened to Bob and if not opens one and sends the message. Note that if this method is never called, a socket connection is never opened. Both the socket connection on Alice's side and the server on Bob's side can be closed by the methods `closeClassicalChannel` and `closeClassicalServer`, respectively. Alternatetively all connections set up by the `CQCCConnection`, including the connection to the CQC server, can be closed by the method `close`.

We emphasise that to have classical communication between the applications, one is not forced to use the built-in functionality realized by the `CQCCConnection`. A standard client/server setup can also be used.

```

# Send corrections to Bob
Alice.sendClassical("Bob",[a,b])

# Stop the connections
Alice.close()

```

2. Code for Bob

As mentioned, Bob will need to know the measurement outcomes from Alice and will therefore setup a server to be able to receive these. Bob will then receive the qubit `qB` which is part of the EPR-pair generated with Alice. By calling the method `recvClassical`, Bob receives

the measurement outcomes that Alice sent. Corrections are then performed, depending on these measurement outcomes. The qubit `qB` will then be in the state Alice prepared, i.e. the state $|+\rangle$. Finally, Bob measures the qubit `qB` which gives 0 or 1 with equal probability.

```
# Initialize the connection
Bob=CQCConnection("Bob")
Bob.startClassicalServer()

# Make an EPR pair with Alice
qB=Bob.recvEPR()

# Receive info about corrections
data=Bob.recvClassical()
message=list(data)
a=message[0]
b=message[1]

# Apply corrections
if b==1:
    qB.X()
if a==1:
    qB.Z()

# Measure qubit
m=qB.measure()
print("Bob meas. out.: {}".format(m))

# Stop the connection
Bob.close()
```

V. OUTLOOK

SimulaQron allows access to simulated quantum internet hardware, enabling application development. Sim-

ulaQron is undergoing continuous development and improvements and new features may be added over time.

CQC itself can be understood as a very low level language by itself, supported directly by SimulaQron, and tailored specifically to the needs and behaviour of quantum internet application programs. At present, CQC is hidden away from view by the Python and C libraries that enable application development at a much higher level. Indeed, programming using the Python CQC library is the fastest way to get started writing a quantum internet application using SimulaQron. It is conceivable that CQC will be integrated into higher level languages directly by a means of a compiler, which produces CQC commands instead of using a dedicated library.

We might also imagine that more convenient higher level programming environments and libraries become available. While the Python CQC library already offers many conveniences, such as dealing with qubits as Python objects, performing specific gates to - for example - generate BB84 states is still a relatively low level approach to programming the quantum internet. Indeed, many protocols depend on exchanging BB84 states, and their creation and processing could in the future be handled by a set of quantum internet software libraries.

Acknowledgments

We thank Lennart Bittel, Ronald Hanson, Peter Humphreys, Norbert Kalb and Arie van Deursen for interesting discussions and feedback. AD and SW were supported by STW Netherlands, and NWO VIDI grant, and an ERC Starting grant.

-
- [1] Charles H Bennett and Gilles Brassard. Quantum Cryptography: Public Key Distribution, and Coin-Tossing. In *Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.
 - [2] Artur K. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67(6):661–663, aug 1991.
 - [3] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. *Theoretical Computer Science*, 560(P1):12–26, dec 2014.
 - [4] Jędrzej Kaniewski and Stephanie Wehner. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics*, 18(5), 2016.
 - [5] Richard Jozsa, Daniel S. Abrams, Jonathan P. Dowling, and Colin P. Williams. Quantum Clock Synchronization Based on Shared Prior Entanglement. pages 0–3, 2000.
 - [6] Andrew M Childs. Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466, nov 2001.
 - [7] A. Kellerer. Quantum telescopes. *Astronomy and Geophysics*, 55(3):1–12, 2014.
 - [8] NetSQUID: Currently in preparation.
 - [9] Damian S. Steiger, Thomas Häner, and Matthias Troyer. ProjectQ: An Open Source Software Framework for Quantum Computing. 2016.
 - [10] Dave Wecker and Krysta M. Svore. LIQUi—>: A Software Design Architecture and Domain-Specific Language for Quantum Computing. 2014.
 - [11] N. Khammassi, I. Ashraf, X. Fu, C.G. Almudever, and K. Bertels. QX: A high-performance quantum computer simulation platform. *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, pages 464–469, 2017.
 - [12] J. R. Johansson, P. D. Nation, and Franco Nori. QuTiP: An open-source Python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 183(8):1760–1772, 2012.
 - [13] Python. <https://www.python.org/>.
 - [14] Twisted. <https://twistedmatrix.com/trac/>.
 - [15] SimulaQron. <http://www.simulaqron.org>.
 - [16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2010.
 - [17] MOOC: Quantum Cryptography on. <https://www.edx.org>.