Cross-platform verification for near-term quantum computers

Domínguez Tubío, Victoria

Cross-platform verification for near-term quantum computers

THESIS

submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE
in
PHYSICS

Author :	Victoria Domínguez Tubío
Student ID :	use \studentid{...} to define
Supervisor :	Jordi Tura i Brugués
2^{nd} corrector :	Vedran Dunjko

Leiden, The Netherlands, August 4, 2021

Cross-platform verification for near-term quantum computers

Victoria Domínguez Tubío

Huygens-Kamerlingh Onnes Laboratory, Leiden University
P.O. Box 9500, 2300 RA Leiden, The Netherlands

August 4, 2021

Abstract

Current quantum devices have shown that they can carry out difficult computations that cannot be mimicked by classical computers, even though the number of qubits available in such devices is in the range of several tens, and without quantum error correction. Several technological challenges need to be overcome to increase the number of qubits of these devices in an effective way. Therefore, how to overcome the scalability problem to construct more powerful quantum computers is a topic of interest. One of the possible solutions is to use distributed quantum computation, where the devices are connected through a coherent link that has a capacity limit of few qubits (e.g. 1). Several protocols work with that setting, including cross-platform verification protocols. They are used to check the correct functioning of the different quantum devices of the distributed setting through the comparison of their generated output states when using the same quantum circuit. In this project, we present three cross-platform verification protocols based on Grover's reflections, namely, they compare the output state of two different quantum devices under the assumption that Alice's device generates the searched state and see if Bob has also generated it. We also show how these protocols could be used in quantum data verification. Finally, we benchmark against the state-of-the-art.

Contents

Chapter 1

Introduction

Quantum computers use the properties of quantum mechanics, such as the superposition of states and their entanglement to perform different algorithms and simulations. Computability-wise, when talking about quantum computers and classical computers, they are equivalent. In other words, the quantum devices can not solve more problems than the classical ones, and vice versa. The promise of quantum computers, as Feynman proposed two decades ago [1], is that they may be more efficient than the classical ones to solve some problems in physics and chemistry [1], [2], for example, the simulation of strongly-correlated systems, given the exponential cost of simulating large quantum systems with classical devices.

1.1 NISQ devices.

Right now, we are in the "stone-age" of quantum computers: the NISQ (Noisy Intermediate Scale Quantum) era. The intermediate scale term refers to the number of qubits available in such devices which are in the range of 50 to a few hundred [2], [3]

The fact that the current quantum computers are noisy implies that the circuits available are shallow, not making it possible to build up circuits with a big amount of gates. This size constraint means that there is also a computational power constraint.

In order to be available to scale up to larger circuits, quantum error correction (QEC) plays a fundamental role. However, the cost of correcting the errors that may show up in a quantum circuit requires many additional physical qubits [4]. Therefore, what we have right now are NISQ devices where the noise is present and unprotected by QEC [3].

How to increase the number of qubits in an effective way in such devices is not a trivial problem. It requires to overcome several technological challenges. Hence, how to go through the scalability problem to construct more powerful quantum computers is a topic of interest. One of the possible solutions is to use distributed quantum computation.

1.2 Distributed quantum computation

Even though NISQ devices are "stone-age" quantum computers, by connecting them through a coherent link with a capacity limit of just a few qubits (e.g. 1 qubit), we can build large-scale devices. The use of different distributed settings is the roadmap of companies like IBM and Google to set up a 1 million qubit quantum compute [5].

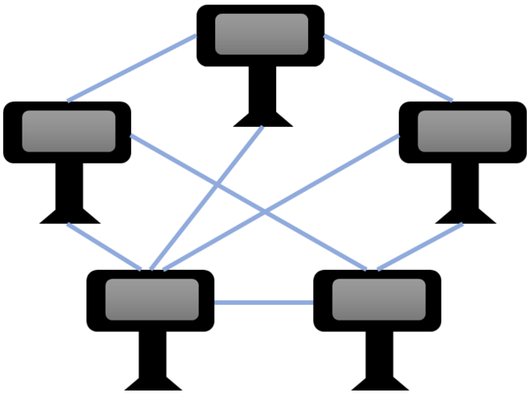


Figure 1.1: *Distributed computation. Several NISQ devices are coherently connected to build up a quantum computer that goes beyond the limit size of a few hundred of qubits of the intermediate scale quantum machines.*

1.3 Cross-platform verification protocols: state-of-the-art.

One of the challenges of these distributed settings is to check their correct functioning, which can be done using cross-platform verification. Verification protocols compare the output states generated by two different quantum devices using the same quantum circuit.

Quantum fidelity is one of the possible measures used to compare the quantum states of interest, ρ_1 and ρ_2. Its mathematical expression is [6]:

$$F(\rho_1, \rho_2) = Tr\left(\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right), \tag{1.1}$$

where we can see that if ρ_1 and ρ_2 are the same quantum states, mixed or pure, the parameter is equal to the unity, $F(\rho_1, \rho_2) = 1$.

The state-of-the-art [7] compute the upper bond of the fidelity, Eq.(1.1):

$$F_{max}(\rho_1, \rho_2) = \frac{Tr(\rho_1\rho_2)}{max\left(Tr\rho_1^2, Tr\rho_2^2\right)}, \tag{1.2}$$

where the value of the fidelity is also 1 when the states are the same.

In a totally quantum protocol, the quantum states would be teleported and compared using a SWAP test. The teleportation of the states would be carried out by a quantum link. By doing so, the fidelity can be computed. Unfortunately, a quantum link teleporting large quantum states between two different devices is not available nowadays [7].

Therefore, the state-of-the-art for cross-device verification requires classical communication between quantum devices.

Brute force tests make use of quantum state tomography to carry out a full classical reconstruction and a subsequent classical comparison of the quantum states. The handicap of this technique is that takes 3^n measurements to determine an arbitrary n-qubit-quantum state [8].

To overcome the scaling problem of the last protocol, Carrasco et.al.[7] propose to compute randomized measurements to get the quantum fidelity of two unknown states, ρ_1 and ρ_2, instead of fully reconstructing them.

A randomized measurement [9] is carried out by applying a random unitary, U, to a quantum circuit followed by the measure of the output on the computational basis. The unitary U can be local (it acts on a certain number of qubits smaller than the system size, n). To do so, instead of using a Haar measure[10] (measure of uniform probability distribution over the unitary group), the whole set of unitaries can be sampled in a quantum 2-design [11], [12] (the properties of the probability distribution over the unitaries of the Haar measure are duplicated in a polynomial of grade 2) , namely they act on the Hilbert space: $\mathbb{C}^2$, $U = \otimes_{k=1}^{n} U_k$, U_k acting on qubit k.

The random measurements have to be done with the same random unitaries on both states, ρ_1 and ρ_2, so there has to be a classical communication channel.

By carrying out several measurements, we can compute the cross-correlation and the autocorrelation of the outcome probabilities, and consequently the trace of the quantum states, ρ_1 and ρ_2 [7], [9].

$$Tr(\rho_i \rho_j) = 2^N \sum_{s,s'} (-2)^{-D[s,s']} \overline{P_U^{(i)}(\vec{s}) P_U^{(j)}(\vec{s}')}, \tag{1.3}$$

where $P_U^{(i)}(\vec{s}) = Tr(U\rho_i U^\dagger |\vec{s}\rangle\langle\vec{s}|)$, $i, j = 1, 2$, $D[s, s']$ is the Hamming distance [13] and $\bar{A}$ is an estimation of A.

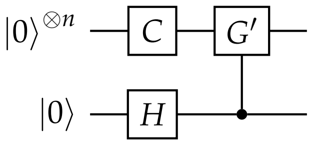
Unfortunately, the scaling of such protocol is 2^{bn}, hence the number of measurements necessary to estimate the fidelity increases exponentially with the subsystem size [7], [9].

On top of that, the construction of an empirical distribution $P(s)$ implies the measurement of the output states. Therefore, ρ_1 and ρ_2 will be destroyed after incompatible measurements (due to the collapse of the wavefunction) and they will have to be generated again.

1.4 Idea.

Keeping in mind the disadvantages of the state-of-the-art aforementioned, we present here a cross-device verification protocol that seeks to overcome them.

We will try to know if the states generated by Alice and Bob are the same without directly measuring them. To do that, it is necessary an ancilla qubit. The basic idea is shown in the following circuit:



$$G = \begin{pmatrix} -1 & 0 & 0 & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ . & & . & & & . \\ . & & & . & & 0 \\ 0 & . & . & . & 0 & 1 \end{pmatrix} \tag{1.4}$$

Figure 1.2: *Cross-platform verification protocol based on Grover search reflections, where $G' = C^{\dagger}GC$, is a reflection with axis $C|0\rangle$.*

Intuitively, the letter G makes reference to the reflection in the Grover search algorithm [14], where the reflection $2(|0\rangle\langle 0|)^{\otimes n} - \mathbb{I}^{\otimes n}$ is the matrix shown in Eq.(1.4).

G' is the G gate expressed in the basis of the states generated by the random gate C, which should be the same for Alice and Bob circuits.

$$|\gamma_i\rangle = C|0\rangle^{\otimes n}, \tag{1.5}$$

where $i = 0, 1, ..2^n - 1$. $|\gamma_i\rangle$ is a basis containing the ideal state $|\gamma_0\rangle$.

$$|\psi_A\rangle = \sum_{i=0}^{2^n-1} \alpha_i |\gamma_i\rangle \qquad (1.6) \qquad |\psi_B\rangle = \sum_{i=0}^{2^n-1} \beta_l |\gamma_l\rangle, \qquad (1.7)$$

where the indices A and B, Eqs.(1.6),(1.7), refer to the states that Alice and Bob generate.

Ideally, the amplitude of the states $|\psi_A\rangle$ and $|\psi_B\rangle$ is $\alpha_i = \delta_{i,0}$ and $\beta_l = \delta_{l,0}$, respectively. So, the desired state is:

$$|\psi_0\rangle = \alpha_0|\gamma_0\rangle = \beta_0|\gamma_0\rangle = |\gamma_0\rangle, \tag{1.8}$$

where $\alpha_0 = \beta_0 = 1$ due to normalization.

For the sake of simplicity, let us start working under the hypothesis that Alice and Bob generate indeed the same state, which is also the desired one, $|\gamma_0\rangle$. Hence, the amplitude of both states is $\alpha_i = \beta_i = \delta_{i,0}$.

Following the different steps indicated in the quantum circuit of Fig.1.2, the output of both circuits takes the form:

- Step 1.
  $$|\gamma_0\rangle|+\rangle, \tag{1.9}$$
  where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.
- Step 2.
  $$\frac{|\gamma_0\rangle|0\rangle + G'|\gamma_0\rangle|1\rangle}{\sqrt{2}} = |\gamma_0\rangle|-\rangle, \tag{1.10}$$
  where $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

On the other hand, if we picture the situation where the state that Bob generates is orthogonal to $|\gamma_0\rangle$, namely $|\psi_B\rangle = \sum_{l=1}^{2^n-1}\beta_l|\gamma_l\rangle$, the output of Bob's circuit will be:

$$\frac{|\psi_B\rangle|0\rangle + G'|\psi_B\rangle|1\rangle}{\sqrt{2}} = |\psi_B\rangle|+\rangle. \tag{1.11}$$

Following the results shown in Eqs.(1.10) and (1.11), we can conclude that if Alice and Bob generate the same state, $|\gamma_0\rangle$, the measurement of the ancilla of both circuits will give the same outcome. However, if the state generated by Alice is $|\gamma_0\rangle$, Eq.(1.6), and the one generated on Bob's circuit is different, the output measured in both circuits is going to be different as well.

On top of that, the fact that we only need to measure the ancilla to compare the states implies that, as long as the tensor product structure in the system-ancilla is preserved, Eqs.(1.10),(1.11), they will not be destroyed after the measurement and that we can measure the ancilla as many times as we want without having to generate again Alice and Bob states.

Specifically, the aim of this protocol is to measure the output of both ancilla together and study its outcome. To do so, a Bell measurement [15] needs to be carried out. Working under the assumption that Alice and Bob generate the state $|\gamma_0\rangle$, Eq.(1.6), and recalling that the output of both circuits is shown in Eq.(1.10), we can obtain the density matrix of both circuits:

$$\rho_{A,syst} = \rho_{B,syst} = \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)|\psi_0\rangle\langle\psi_0| \tag{1.12}$$

By tracing over the system, the density matrices of the ancilla are calculated:

$$\rho_A = \rho_B = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \tag{1.13}$$

Hence, the density matrices of the system computed by both ancilla is:

$$\rho_A \otimes \rho_B = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{1.14}$$

Carrying out the Bell measurements with the following states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.15}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{1.16}$$

leads to the results:

$$\langle\phi^+|\rho_A \otimes \rho_B|\phi^+\rangle = \frac{1}{2} \tag{1.17}$$

$$\langle\phi^-|\rho_A \otimes \rho_B|\phi^-\rangle = 0 \tag{1.18}$$

On the other hand, if Alice generates $|\gamma_0\rangle$ and Bob $|\psi_B\rangle = \sum_{l=1}^{2^n-1}\beta_l|\gamma_l\rangle$. The output of Bob's circuit would be the one shown in Eq.(1.11) and the density matrix of the ancilla:

$$\rho_B = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \tag{1.19}$$

Analogously to the procedure performed in the previous case, the density matrix of both ancillas is:

$$\rho_A \otimes \rho_B = \frac{1}{4}\begin{pmatrix} 1 & \cdots & -1 \\ \vdots & & \vdots \\ -1 & \cdots & 1 \end{pmatrix} \tag{1.20}$$

And the result of the Bell measurements:

$$\langle \phi^+ | \rho_A \otimes \rho_B | \phi^+ \rangle = 0 \tag{1.21}$$

$$\langle \phi^- | \rho_A \otimes \rho_B | \phi^- \rangle = \frac{1}{2}, \tag{1.22}$$

Finally, combining the results shown when Alice and Bob generate the desired state, Eqs.(1.17),(1.18), and the ones obtained when Bob generate $|\psi_B\rangle \neq |\gamma_0\rangle$, Eqs.(1.21),(1.22); we can infer that in the situation where Bob is dealing with a noisy circuit:

$$|\psi_B\rangle = \beta_0 |\gamma_0\rangle + \sum_{l=1}^{2^n-1} \beta_l |\gamma_l\rangle, \tag{1.23}$$

where $|\beta_l| << |\beta_0|$, the value of the Bell measurements will be:

$$\langle \phi^+ | \rho_A \otimes \rho_B | \phi^+ \rangle < \frac{1}{2} \tag{1.24}$$

$$\langle \phi^- | \rho_A \otimes \rho_B | \phi^- \rangle > 0 \tag{1.25}$$

Therefore, by carrying out a Bell measurement on both ancillas, we can conclude if Bob and Alice have generated the desired state or not.

Nevertheless, the construction of G carries some undesired errors that can be avoided. In the case of being working with 2 qubits (without taking into account the ancilla), the circuit to compute the reflection in the computational basis, $2|00\rangle\langle 00| - \mathbb{I}$, is the following one [15]:

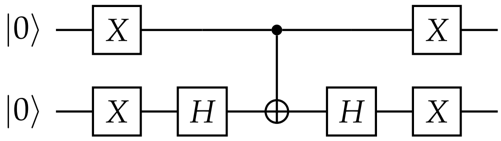


Figure 1.3: *Quantum circuit that computes the reflection* $2(|0\rangle\langle 0|)^{\otimes n} - \mathbb{I}^{\otimes n}$ *(the operation called G), for* $n = 2$.

Fig.1.3 shows that to construct G is necessary a $CNOT$ gate. The former gate in a system of 2 qubits does not suppose a problem to implement it. However, when working with n qubits, we will have a $C^{\otimes(n-1)}NOT$ gate. Controlling $n-1$ should be avoided in NISQ devices due to the large, $O(n)$, gate complexity it demands [16].

In this project we show three cross-platform verification protocols based on the idea just explained. To overcome the depth complexity that the latter requires, the controlled-unitaries used in the quantum circuits, Fig.1.2, of the following protocols are constructed using Z gates, Z_ϕ gates [15], [17] or Haar gates [10]. We study how to implement them and how the number of experimental runs scales with the system size. Additionally, we explain that besides being useful to check the correct functioning of the different devices of the quantum distributed computation, they can be used in quantum data verification [18]. Finally, the protocols studies are compared with the state-of-the-art [7].

Chapter 2

Cross-platform verification protocols

Combining the need of designing a new cross-platform verification protocol and the basic idea of the one explained in the previous chapter, gives as a result three new possible protocols that we present in this section. In other words, they are used to compare Alice's and Bob's generated states and check if they are the same and equal to the searched one, $|\gamma_0\rangle$, Eq.(1.6). Specifically, they are designed to work under the assumption that Alice generates the latter and see if Bob has also generated it. Additionally, all of them seek to have a different eigenvalue between the searched state and the rest, $|\psi_i\rangle$, $i \neq 0$. Therefore, when performing the Bell measurements, if Alice and Bob generate $|\gamma_0\rangle$ the outcome will not be the same that when generating any other state.

The idea behind the first one is to use a Z gate, [15], [17], on different qubits of Alice's and Bob's circuits, leading to two non-identical controlled-unitaries, $C - U_A$ and $C - U_B$ [15], [17]. However, this protocol only works when Bob's unitary, U_B, changes every time we measure. In other words, the Z gate must be applied on a different qubit on each measurement.

In order to optimize the previous protocol, the following uses different controlled unitaries constructed by applying n different Z_ϕ gates [15] to the n qubits of the circuit, where ϕ is a random phase different on each qubit. In this way, the eigenvalue of each eigenstate $|\gamma_i\rangle$ is different from each other, being able to distinguish $|\gamma_0\rangle$ from the rest with just a single circuit configuration.

Finally, the last protocol also uses random values as the previous one, but this time the unitaries are a special construction of Haar gates [10], where the eigenvalue of $|\gamma_0\rangle$ is 1 and the eigenvalues of the rest of the states are random values.

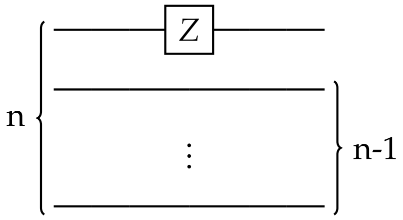
2.1 Z gates

A Z gate, key in this protocol, is a one qubit gate and one of the Pauli matrices (σ_z) [15]. Additionally, is a specific case of Z_ϕ rotation gate, where $\phi = 180°$.

$$Z_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \tag{2.1}$$

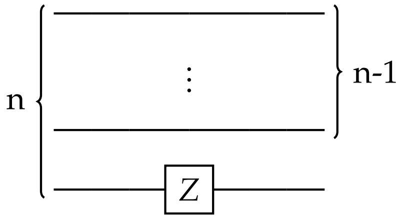
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.2}$$

As we can not implement G without a large amount of gates, we can instead use the Z gate and implement different unitaries like the ones shown below:



$$U' = Z \otimes \mathbb{I}_{(n-1)} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & -1 & & \\ & & & \ddots & \\ & & & & -1 \end{pmatrix} \qquad (2.3)$$

Figure 2.1: *Alternative unitary to implement instead of the Grover search unitary, G, using a Z gate on the first qubit.*



$$U'' = \mathbb{I}_{(n-1)} \otimes Z = \begin{pmatrix} 1 & & & & \\ & -1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & -1 \end{pmatrix} \qquad (2.4)$$

Figure 2.2: *Alternative unitary to implement instead of the Grover search unitary, G, using a Z gate on the last qubit.*

To move the spins where we need, we add X gates [15], [17] to the beginning and to the end of each of the wires of the circuits shown in Figs.2.1,2.2, and we implement the unitaries U'_X and U''_X. The eigenvalues of these last unitaries are inverted with respect to U' and U'', i.e., the first eigenvalue of U'_X is the last of U', the second of U'_X, the second last of U', and so on. By using U'_X and U''_X, the eigenvalue of $|\gamma_0\rangle$ is minus one, same value as the one shown in the G gate, Eq.(1.4), of the previous chapter.

Nevertheless, it does not matter if the eigenvalue of the searched state has a positive or a negative sign, the goal is that its eigenvalue is different from the rest. Therefore, for the sake of simplicity and trying to avoid extra errors by adding unnecessary gates, we will work with the unitaries U' and U'', Eqs.(2.3),(2.4).

Fixing our attention on the aforementioned unitaries, we can see that there are eigenvectors that share the eigenvalue of the searched state. This would lead to the problem of not being able to know if Alice and Bob have really generated the latter. Let us check this out by computing a Bell measurement on the ancilla of both circuits.

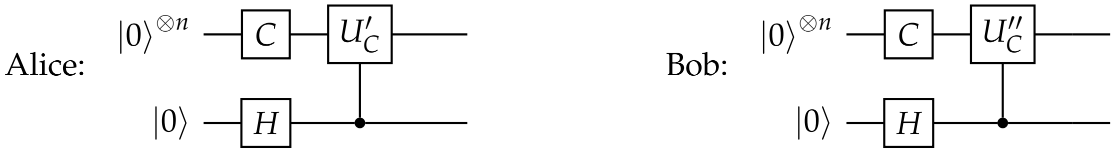


Figure 2.3: *Alice's (left) and Bob's (right) circuits for the implementation of a cross-platform verification algorithm using Z gates on the controlled-unitaries, U'_C, U''_C, being the Z gate applied on a different qubit on each unitary.*

The controlled unitaries, $C - U'_C$ and $C - U''_C$, of Alice's and Bob's circuits, Fig.2.3, are constructed using U' and U'', Eqs.(2.3),(2.4), and a change of basis, $U'_C = C^{\dagger}U'C$, $U''_C = C^{\dagger}U''C$. Therefore, they work on the basis of the output states of gate C. From now on, for the sake of simplicity in the notation, when calculating the output states of both circuits, the unitaries U' U'' will be already in the desired basis, so u'_{ii} and u''_{ll} will be the eigenvalues of $|\gamma_i\rangle$, $|\gamma_l\rangle$ respectively.

$$|\Phi_{AL}\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle U'|\psi\rangle\right) = \frac{1}{\sqrt{2}}\sum_{i=0}^{2^n-1}\left(|0\rangle\alpha_i|\gamma_i\rangle + |1\rangle\alpha_i u'_{ii}|\gamma_i\rangle\right) \tag{2.5}$$

$$|\Phi_{Bob}\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle U''|\psi\rangle\right) = \frac{1}{\sqrt{2}}\sum_{l=0}^{2^n-1}\left(|0\rangle\beta_l|\gamma_l\rangle + |1\rangle\beta_l u''_{ll}|\gamma_l\rangle\right), \tag{2.6}$$

where the basis used has been already shown in the previous chapter, Eqs. (1.5), (1.6) and (1.7).

In order to perform a Bell measurement, we need the density matrix of the output of both circuits:

$$\rho_{A,syst} = |\Phi_{Al}\rangle\langle\Phi_{Al}| = \frac{1}{2}\sum_{i,j}\left(|0\rangle + u'_{ii}|1\rangle\right)\Big(\langle 0| + \bar{u}'_{jj}\langle 1|\Big)\,\alpha_i\bar{\alpha}_j|\gamma_i\rangle\langle\gamma_j| \tag{2.7}$$

$$\rho_{B,syst} = |\Phi_{Bob}\rangle\langle\Phi_{Bob}| = \frac{1}{2}\sum_{l,k}\left(|0\rangle + u''_{ll}|1\rangle\right)\left(\langle 0| + \bar{u}''_{kk}\langle 1|\right)\beta_l\bar{\beta}_k|\gamma_l\rangle\langle\gamma_k| \tag{2.8}$$

By tracing out over the system, we get the density matrix of each of the ancilla:

$$\rho_A = Tr_{syst}(\rho_{A,syst}) = \frac{1}{2}\sum_i|\alpha_i|^2\begin{pmatrix}1 & u'_{ii}\\ u'_{ii} & 1\end{pmatrix} \tag{2.9}$$

$$\rho_B = Tr_{syst}(\rho_{B,syst}) = \frac{1}{2}\sum_l|\beta_l|^2\begin{pmatrix}1 & u''_{ll}\\ u''_{ll} & 1\end{pmatrix}, \tag{2.10}$$

where we applied that $\bar{u}^{'}_{ii} = u^{'}_{ii}$ and $\bar{u}''_{ll} = u''_{ll}$.

Before carrying out with the calculations, let's work under the usual assumption that the state generated by Alice is $|\psi_0\rangle$, i.e, the amplitude of the state is $\alpha_i = \delta_{i,0}$. Considering that $u'_{00} = 1$:

$$\rho_{A_0} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, \tag{2.11}$$

and the density matrix of the system of both ancillas is:

$$\rho_{A_0}\otimes\rho_B = \frac{1}{4}\sum_i|\beta_l|^2\begin{pmatrix}1 & . & . & u''_{ll}\\ . & . & . & .\\ . & . & . & .\\ u''_{ll} & . & . & 1\end{pmatrix}, \tag{2.12}$$

where just the terms needed to perform the Bell measurements are shown, and the outputs of the aforementioned measurements are:

$$\langle \phi^{+} | \rho_A \otimes \rho_B | \phi^{+} \rangle = \frac{1}{4} \sum_{l} |\beta_l|^2 (1 + u''_{ll}) \tag{2.13}$$

$$\langle \phi^{-} | \rho_A \otimes \rho_B | \phi^{-} \rangle = \frac{1}{4} \sum_{l} |\beta_l|^2 (1 - u''_{ll}) \tag{2.14}$$

In the ideal case, where Bob generates also $|\psi_0\rangle$, $u''_{00} = 1$, the former expressions, Eqs.(2.13),(2.14), have the following values:

$$\langle \phi^{+} | \rho_A \otimes \rho_B | \phi^{+} \rangle = \frac{1}{2} \tag{2.15}$$

$$\langle \phi^{-} | \rho_A \otimes \rho_B | \phi^{-} \rangle = 0, \tag{2.16}$$

same result as the ones obtained in the previous chapter1, Eqs.(1.17), (1.18).

Recalling now the shape of U'', Eq.(2.6), unitary of Bob's circuit, we can appreciate that: $u''_{ll} = 1$, if l is an even number, $l = 2n$; and $u''_{ll} = -1$, if l is an odd number, $l = 2n + 1$. Therefore, if Bob instead of generating $|\psi_0\rangle$, generates $|\psi_{2l}\rangle = \beta_{2l} |\gamma_l\rangle$, we can not distinguish the former states when carrying out a Bell measurement.

The previous mishap can be solved by changing Bob's controlled-gate every time we measure, in such a way that in the intersection space between all the unitaries the only eigenvalue equal to 1 is u''_{00}. To do so, we need to apply n controlled-gates of the form: $U''_0 = Z \otimes \mathbb{I}_{(n-1)}$; $U''_1 = \mathbb{I} \otimes Z \otimes \mathbb{I}_{(n-2)}$ ... $U''_n = \mathbb{I}_{(n-1)} \otimes Z$, being n the number of qubits.

As a final remark, the gates used do not need to be Z gates, since the goal is in principle apply a different phase between $|\psi_0\rangle$ and $|\psi_i\rangle$. Therefore, any Z_ϕ works in this algorithm. Additionally, the aforementioned eigenvalues do not have to be real anymore, $u'_{ii} \neq \bar{u}'_{ii}$ $u''_{ll} \neq \bar{u}''_{ll}$, and Eqs.(2.14),(2.13) take the form:

$$\langle \phi^{+} | \rho_A \otimes \rho_B | \phi^{+} \rangle = \frac{1}{4} \sum_{l} |\beta_l|^2 (1 + Re(u''_{ll})) \tag{2.17}$$

$$\langle \phi^{-} | \rho_A \otimes \rho_B | \phi^{-} \rangle = \frac{1}{4} \sum_{l} |\beta_l|^2 (1 - Re(u''_{ll})) \tag{2.18}$$

2.1.1 Hypothesis test

The correct estimation of the values of the Bell measurements requires to measure the ancillas of Bob's and Alice's circuits more than once. To know how many times, we need to compute a hypothesis test.

For the sake of simplicity, we will start by showing the ideal case, where there is no noise in any of the circuits, and Bob prepares and eigenstate of the unitary, $|\gamma_j\rangle$, i.e, there is not yet a superposition of different states, $|\psi_B\rangle$, Eq.(1.7).

- if $\hat{\mu} = 0$, we accept the hypothesis that "Bob generates $|\gamma_0\rangle$". We will call it the null hypothesis, H_0.
- if $\hat{\mu} \neq 0$, we reject the hypothesis. It is the alternative hypothesis, H_a.

Where $\mu = \langle\phi^-|\rho_A \otimes \rho_B|\phi^-\rangle$, $\hat{\mu} := \sum_{i=1}^{n_e} X_i/n_e$, being X_i random variables.

The total number of measurements needed to carry out this protocols to have an acceptable value of the expectation value of the Bell measurements is defined by:

$$N = k \times n_e, \tag{2.19}$$

where k is the number of times Bob changes the unitary in his circuit and n_e is the number of times the output is measured in a certain circuit configuration, i.e. n_e is the number of experimental runs computed for each k. As we are dealing now with the ideal case, where the noise is not considered, $n_e = 1$.

To compute k we calculate the error of the first kind. The latter implies to accept H_0 when it is not true, i.e, to accept that Bob generates $|\gamma_0\rangle$ when he does not.

$$P(\text{ accept } H_0|H_a \text{ is true }) := \delta \tag{2.20}$$

Let us picture that in the first circuit configuration, Bob's unitary is $\mathbb{I}_{n-1} \otimes Z$. Recalling that he prepares an eigenstate $|\gamma_j\rangle$, the probability that the eigenvalue of $|\gamma_j\rangle$ is 1 is $1/2$. One of the former eigenvalues corresponds to the eigenvector $|\gamma_0\rangle$, i.e. the searched state. Hence, the probability of making an error of the first kind is:

$$\delta = \frac{1}{2} - \frac{1}{2^n}. \tag{2.21}$$

Now, in the second circuit configuration, Bob's unitary is $\mathbb{I} \otimes Z \otimes \mathbb{I}_{n-2}$, and the probability that the eigenvalue of $|\gamma_j\rangle$ is +1 in both measurements, i.e. in the intersection space between the two unitaries, is $1/4$. Therefore, after two measurements the probability of accepting wrongly that Bob also generated $|\gamma_0\rangle$ is:

$$\delta = \frac{1}{4} - \frac{1}{2^n}. \tag{2.22}$$

When carrying out the third circuit configuration with another unitary where the Z gate is on another qubit, the probability that the eigenvalue of $|\gamma_j\rangle$ is 1 in the intersection state between the unitaries is $1/8 = \frac{1}{2^n}$, where $n = 3$.

Therefore, we can appreciate how the probability of committing an error of the first kind decreases exponentially with the number of qubits, n. As we are not considering noise, after $N = k = n$ measurements, $\delta = 0$, Eq.(2.23).

$$\delta = \frac{1}{2^n} - \frac{1}{2^n} = 0. \tag{2.23}$$

Generally, the hypothesis H_0 is accepted with a certain confidence interval. In other words, if we want to be right at least 90% of the times that we say that Bob has generated the same state as Alice, we set $\delta' = 0.1$.

So, what is the number of different circuit configurations, k, needed to compute for a certain δ'? In the next section, we obtain the upper limit of k by picturing the worst case, where Bob wants to fool Alice and commit an error of the first kind.

Worst case scenario

Usually, we will have that the probability of accepting H_0 when H_a is true is of the form:

$$P(\text{ accept } H_0|H_a \text{ is true }) = \frac{1}{2^k} - \frac{1}{2^n} \leq \delta'. \tag{2.24}$$

After some algebra:

$$\frac{1}{2^k} \leq \delta' + \frac{1}{2^n} \longrightarrow -klog(2) \leq log\left(\delta' + \frac{1}{2^n}\right) \longrightarrow k \geq \frac{log\left(\frac{1}{\delta' + \frac{1}{2^n}}\right)}{log(2)}$$

$$k \geq log_2\left(\frac{1}{\delta' + \frac{1}{2^n}}\right) \tag{2.25}$$

We can appreciate that if $\delta' = 0$, $k \geq n$, in concordance with the result shown in Eq.(2.23). Additionally, if $\delta' = 1/poly(n)$, then $1/2^n$ is negligible and $k \geq log_2(n)$. So k has a logarithmic dependence with the system size, n, if we choose $\delta' = 1/poly(n)$.

Noisy states

Besides considering that Bob can generate any other state than $|\gamma_0\rangle$, we may also think about the possibility that he generates a noisy $|\psi_0\rangle$, Eq.(1.23), due to a systematic mistake in the circuit. Therefore, the output of the Bell measurement will be:

$$\langle\phi^+|\rho_A \otimes \rho_B|\phi^+\rangle \leq \frac{1}{2} \tag{2.26}$$

$$\langle\phi^-|\rho_A \otimes \rho_B|\phi^-\rangle \geq 0, \tag{2.27}$$

where the inequality holds for the case of Bob not generating $|\gamma_0\rangle$ perfectly.

On top of that, the current quantum devices are NISQ devices, which implies that it is not just Bob the one generating noisy states. In this case, we will consider that the expectation value of the Bell measurements is:

$$\mathbb{E}(\langle\phi^-|\rho_A \otimes \rho_B|\phi^-\rangle) = \alpha \approx 0, \tag{2.28}$$

which shows that both, Alice and Bob, are working with NISQ devices.

To check whether Bob is generating a noisy state due to, for instance, an error in the implementation of the gates, or if he is generating the same state as Alice, we need to carry out a hypothesis test. On top of that, we need to balance between the two possible situations of Bob being a bit clumsy and Bob trying to fool Alice (worst case scenario). To do that, we consider a regime of possible values for the outcome of the Bell measurements.

- If $|\hat{\mu} - \mathbb{E}(\mu)| < \varepsilon$, we accept the hypothesis that Bob generates the same state as Alice. This is the null hypothesis, H_0.
- If $|\hat{\mu} - \mathbb{E}(\mu)| \geq \varepsilon$, we reject the hypothesis. It is the alternative hypotehsis, H_a

Where $\mu = \langle\phi^-|\rho_A \otimes \rho_B|\phi^-\rangle$, $\hat{\mu} := \sum_{i=1}^{n_e} X_i/n_e$, and ε is the precision that we want to reach between the measured outcome and the expected one. In other words, ε is the parameter that expresses how clumsy can be Bob generating his state.

The computation of the error of the second kind gives the number of measurements, n_e, needed to accept the previous hypothesis with a certain confidence interval. An error of the second kind involves accepting H_a when H_0 is true. We seek that the probability of committing an error of the second kind is smaller than a certain δ''.

$$P(|\hat{\mu} - \mathbb{E}(\mu)| \geq \varepsilon) \leq \delta'' \tag{2.29}$$

Since X_i is bounded and a Bernoulli random variable [19] of parameter $p = \alpha$, being α the theoretical value of the expectation value of the Bell measurement (Eq.(2.28)), Eq.(2.29) is basically the Chernoff- Hoeffding's inequality [20]:

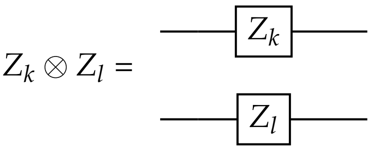
$$P(|\hat{\mu} - \mathbb{E}(\mu)| \geq \varepsilon) \leq 2e^{-2n_e\varepsilon^2} \tag{2.30}$$

Combining Eqs.2.29 and 2.30:

$$n_e \geq log(2/\delta'')/2\varepsilon^2 \propto O(\varepsilon^{-2}) \tag{2.31}$$

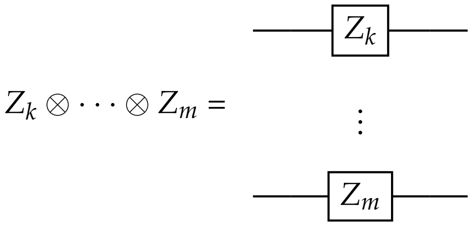
2.2 Random phase

As it was mentioned in the previous section 2.1, it does not matter if the gates used are Z gates or any Z_ϕ gates. The goal is to use a gate that applies a different phase between $|\gamma_0\rangle$ and the rest of the states $|\gamma_i\rangle$, $i \neq 0$. This protocol seeks to use just one circuit configuration and not the k needed in the previous one to have a reliable value of the Bell measurements. To do that, the controlled unitaries of this protocols are constructed using n different Z_ϕ rotation gates, being n the number of qubits and ϕ a random phase, on each qubit of Alice's and Bob's circuits. By doing so, the eigenvalue of the searched state will be 1 and the rest of them $e^{i\phi_i}$, being ϕ_i the phase of the eigenvalue u_{ii} of the state $|\gamma_i\rangle$, $i = 1...2^n - 1$.



$$Z_k \otimes Z_l = \begin{pmatrix} 1 & & & \\ & e^{il} & & \\ & & e^{ik} & \\ & & & e^{i(l+k)} \end{pmatrix} \qquad (2.32)$$

Figure 2.4: *Cross-platform verification protocol using Z rotation gates with a random and different phase each for the case of n=2.*



$$Z_k \otimes \cdots \otimes Z_m = \begin{pmatrix} 1 & & & \\ & e^{im} & & \\ & & \ddots & \\ & & & e^{i\sum_{i=0}^{n-1}\phi_i} \end{pmatrix} \qquad (2.33)$$

Figure 2.5: *Cross-platform verification protocol using Z rotation gates with a random and different phase each for the case of n qubits.*

Let us picture first the case of $n = 2$ qubits followed by the general case of n qubits.

Figs.2.4 and 2.5 shows that by applying different Z rotation to the different qubits, the resultant controlled unitary applies different eigenvalues to the different eigenvectors. However, we need to be careful with the value of the different phases, $\phi_i \neq 2n\pi$, $n = 0, 1, 2...$, $i \neq 0$ and their sum, $e^{i\sum_{i=0}^{n-1}\phi_i} \neq 2n\pi$, to avoid that a random state $|\gamma_i\rangle$ has the same eigenvalue as $|\gamma_0\rangle$.

2.2.1 Considerations on the hypothesis test

The main difference between the number of measurements of the previous protocol using Z gates and this one, is found in k, i.e. the different circuit configurations needed to apply to be able to accept or reject the hypothesis that Bob also generates $|\gamma_0\rangle$ with a small probability of committing an error of the first kind. The randomness of the different phases used in the controlled unitary of the latter protocol, makes the idea of Bob generating a state with the same eigenvalue as $|\gamma_0\rangle$ a hard task. In the worst case scenario, he can generate a state whose phase in the $C - Z_\phi$ gate is really close to 2π. On the other hand, the randomness of the phases previously mentioned, makes the previous situation not highly probable. Therefore, when working with Z_ϕ we can guess that the number of different circuit configurations required to know if Bob has generated $|\gamma_0\rangle$ is going to be $k' < k$.

Additionally, taking into account that Alice and Bob work with NISQ devices, we need to repeat several times the experimental runs with each circuit configuration to have an acceptable estimation of the expected values of the Bell measurements, up to a give precision ε. The procedure to get that number of experimental runs is the same that the one described in section 2.1.1 and the number of measurements needed to estimate the value of the Bell measurement to a given precision to a given probability is $N = k' \times n_e$, Eq.(2.31).

2.3 Haar gates

Instead of applying n different Z_ϕ gates with random phases, we can check if Alice and Bob have generated the same state $|\gamma_0\rangle$ by using Haar unitaries [10] (random gates) as controlled gates. Such gates must meet the following conditions:

$$U_A \text{ s.t. } U_A|\gamma_0\rangle = |\gamma_0\rangle \tag{2.34}$$

$$U_B \text{ s.t. } U_B|\gamma_0\rangle = |\gamma_0\rangle \tag{2.35}$$

Therefore, the Haar unitaries should be of the form shown in Eqs.(2.36),(2.37).

$$U_A = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & u^{\perp}_{A,11} & \cdots & u^{\perp}_{A,12^n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & u^{\perp}_{A,2^n1} & \cdots & u^{\perp}_{A,2^n2^n} \end{pmatrix} \tag{2.36}$$

$$U_B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & u^{\perp}_{B,11} & \cdots & u^{\perp}_{B,12^n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & u^{\perp}_{B,2^n1} & \cdots & u^{\perp}_{B,2^n2^n} \end{pmatrix} \tag{2.37}$$

Following the same procedure as in chapter 1 and 2.1, Alice's and Bob's circuits are shown in Fig.2.6, where U_A and U_B are already in the C-basis, and the output of Alice's circuit is:

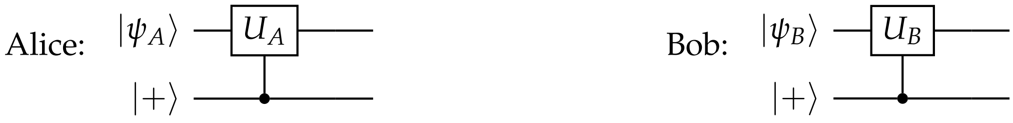


Figure 2.6: *Alice's (left) and Bob's (right) circuits when the controlled gates used are Haar unitaries.*

$$\frac{1}{\sqrt{2}}\left(|\psi_A\rangle|0\rangle + U_A|\psi_A\rangle|1\rangle\right) = \frac{1}{\sqrt{2}}\left(\alpha_0|\gamma_0\rangle(|0\rangle+|1\rangle) + \sum_{i>0}\alpha_i\left(|\gamma_i\rangle|0\rangle + U_A^{\perp}|\gamma_i\rangle|1\rangle\right)\right), \tag{2.38}$$

where the last equation, Eq.(2.38), is equivalent to $|\Phi_{A,syst}\rangle$.

As usual, we calculate now the reduced density matrix, ρ_A. To do so, we first obtain the density matrix of the ancilla and the system, $\rho_{A,syst} = |\Phi_{A,syst}\rangle\langle\Phi_{A,syst}|$, and trace over the system part, considering that $\sum_i |\gamma_i\rangle$ in an orthonormal basis, so $|\gamma_i\rangle\langle\gamma_j| = \delta_{i,j}$.

$$\rho_A = Tr_{syst}(\rho_{A,syst}) = \frac{1}{2}|\alpha_0|^2\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} + \frac{1}{2}\sum_{i>0}|\alpha_i|^2\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \frac{1}{2}\sum_{i,j>0}\begin{pmatrix}0 & \bar{c_{ij}}\\ c_{ij} & 0\end{pmatrix}, \tag{2.39}$$

where $c_{ij} = \alpha_i\bar{\alpha}_j\langle\gamma_j|U_A^{\perp}|\gamma_i\rangle$, and $\bar{c_{ij}}$ is the complex conjugate.

Arranging a bit Eq.(2.39), we get to the expression:

$$\rho_A = \frac{1}{2}\begin{pmatrix} |\alpha_0|^2 + \sum_{i>0}|\alpha_i|^2 & |\alpha_0|^2 + \sum_{i,j>0}\bar{c}_{ij} \\ |\alpha_0|^2 + \sum_{i,j>0}c_{ij} & |\alpha_0|^2 + \sum_{i>0}|\alpha_i|^2 \end{pmatrix} \tag{2.40}$$

Analogously, the reduced density matrix for the ancilla of Bob's circuit is:

$$\rho_B = \frac{1}{2}\begin{pmatrix} |\beta_0|^2 + \sum_{l>0}|\beta_l|^2 & |\beta_0|^2 + \sum_{l,k>0}\bar{b}_{lk} \\ |\beta_0|^2 + \sum_{l,k>0} b_{lk} & |\beta_0|^2 + \sum_{l>0}|\beta_l|^2 \end{pmatrix}, \tag{2.41}$$

where $b_{lk} = \beta_l\bar{\beta}_k\langle\gamma_k|U_B^{\perp}|\gamma_l\rangle$, and $\bar{b}_{lk}$ is the complex conjugate.

Finally, the density matrix of both ancilla is:

$$\rho_A \otimes \rho_B = \frac{1}{4}\begin{pmatrix} A_{00}B_{00} & \cdots & A_{01}B_{01} \\ \vdots & \cdots & \vdots \\ A_{10}B_{10} & \cdots & A_{11}B_{11} \end{pmatrix}, \tag{2.42}$$

where $A_{00} = A_{11} = \left(|\alpha_0|^2 + \sum_{i>0}|\alpha_i|^2\right)$, $B_{00} = B_{11} = \left(|\beta_0|^2 + \sum_{i>0}|\beta_l|^2\right)$, $A_{10} = |\alpha_0|^2 + \sum_{i,j>0} c_{ij}$, $A_{01} = \bar{A}_{10}$, $B_{10} = |\beta_0|^2 + \sum_{l,k>0} b_{lk}$, and $B_{01} = \bar{B}_{10}$.

Using the terms of the resultant density matrix, Eq.(2.42), we get the expectation value of the Bell measurements:

$$\langle\phi^+|\rho_A \otimes \rho_B|\phi^+\rangle = \frac{1}{8}(2A_{00}B_{00} + A_{10}B_{10} + \overline{A_{10}B_{10}}) = \frac{1}{4}\left(A_{00}B_{00} + Re(A_{10}B_{10})\right) \tag{2.43}$$

After some algebra:

$$\langle\phi^+|\rho_A \otimes \rho_B|\phi^+\rangle = \frac{1}{2}\Gamma + \frac{1}{4}(\Delta + \eta), \tag{2.44}$$

where:

$$\Gamma = |\alpha_0|^2|\beta_0|^2, \tag{2.45}$$

$$\Delta = |\alpha_0|^2\sum_{l>0}|\beta_l|^2 + |\beta_0|^2\sum_{i>0}|\alpha_i|^2 + \sum_{i,l>0}|\alpha_i|^2|\beta_l|^2, \tag{2.46}$$

$$\eta = Re(|\alpha_0|^2\sum_{l,k>0} b_{lk} + |\beta_0|^2\sum_{i,j} c_{ij} + \sum_{i,j,l,k>0} c_{ij}b_{lk}. \tag{2.47}$$

Repeating the same procedure, the expectation value of the $|\phi^-\rangle$ Bell state is:

$$\langle\phi^-|\rho_A \otimes \rho_B|\phi^-\rangle = \frac{1}{8}(2A_{00}B_{00} - A_{10}B_{10} - \overline{A_{10}B_{10}}) = \frac{1}{4}\left(A_{00}B_{00} - Re(A_{10}B_{10})\right) \tag{2.48}$$

Analogously to the expected Bell measurement with $|\phi^+\rangle$:

$$\langle \phi^- | \rho_A \otimes \rho_B | \phi^- \rangle = \frac{1}{4} (\Delta - \eta) \tag{2.49}$$

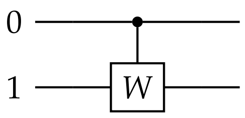
If Alice and Bob generate the state $|\gamma_0\rangle$, Eq.(1.6), then:

$$\langle \phi^+ | \rho_A \otimes \rho_B | \phi^+ \rangle = 1/2 \text{ and } \langle \phi^- | \rho_A \otimes \rho_B | \phi^- \rangle = 0, \tag{2.50}$$

same values for the Bell measurements as the ones computed with the previous algorithms, chapters 1, 2.1.

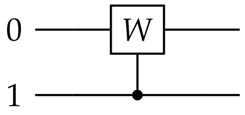
2.3.1 Construction of the Haar gate

The effective implementation we propose of the Haar gates shown in Eqs.(2.36),(2.37) need the use of several controlled gates. Let us start then by explaining them.



$$C_0 - W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & w_{00} & w_{01} \\ 0 & 0 & w_{10} & w_{11} \end{pmatrix} \tag{2.51}$$

Figure 2.7: *2-qubit controlled gate, where W is a single qubit gate, and $C - W$ is the controlled gate of W. The numbers on the left side of the circuit indicates which qubit is the control one, namely the first or the last one. In this case the control qubit is the first one, implying that when its $|1\rangle$, the unitary W is applied on the second qubit.*



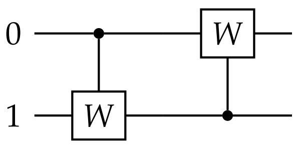
$$C_1 - W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & w_{00} & 0 & w_{01} \\ 0 & 0 & 1 & 0 \\ 0 & w_{10} & 0 & w_{11} \end{pmatrix} \tag{2.52}$$

Figure 2.8: *2-qubit controlled gate, where W is a single qubit gate, and $C - W$ is the controlled gate of W. The numbers on the left side of the circuit indicates which qubit is the control one, namely the first or the last one. In this case the control qubit is the last one, implying that when its $|1\rangle$, the unitary W is applied on the first qubit.*

Figs.2.7 and 2.8 show 2-qubits controlled gates with different control qubits. In Fig.2.7, the control qubit is the first one, meaning that if its state is $|1\rangle$ the single-qubit unitary W is applied to the second qubit, Eq.(2.53). On the other hand, in Fig.2.8 the control qubit is the second one implying the operations shown in Eq.(2.54).

$$|00\rangle \to |00\rangle \;;\; |01\rangle \to |01\rangle \;;\; |10\rangle \to |1\rangle \otimes W|0\rangle \;;\; |11\rangle \to |1\rangle \otimes W|1\rangle \tag{2.53}$$

$$|00\rangle \to |00\rangle \;;\; |01\rangle \to W|0\rangle \otimes |1\rangle \;;\; |10\rangle \to |10\rangle \;;\; |11\rangle \to W|1\rangle \otimes |1\rangle \tag{2.54}$$



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & w_{00} & w_{01}w_{10} & w_{01}w_{11} \\ 0 & 0 & w_{00} & w_{01} \\ 0 & w_{10} & w_{10}w_{11} & w_{11}^2 \end{pmatrix} \tag{2.55}$$

***Figure 2.9:** Construction of the Haar gates $U_{A,B}$, Eqs.(2.36),(2.37) for the case of 2 qubits. The matrix product of the 2 controlled gates gives as a result a matrix $2^2 \times 2^2$ where the 00 element is 1 and the other elements of the fist row and first column are 0. The elements of the remaining columns and rows are a combination of zeros and random values. By computing several times the configuration shown in the left side of the figure, the resulting gate is the searched Haar gate.*

By repeating several times the configuration shown in Fig.2.9, i.e. computing the matrix product of Eq.(2.55) more than once, and working under the supposition that the different elements of the single qubit gate, W, are random (w_{00}, w_{01}, w_{10} and w_{11} are random values), the Haar gates used in the previous protocol, 2.3 can be implemented.

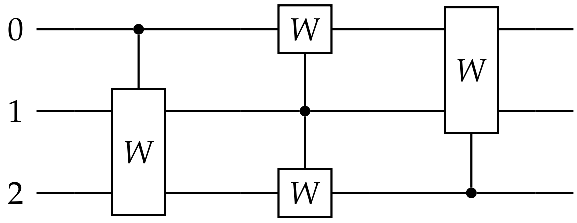


***Figure 2.10:** Construction of the Haar gates $U_{A,B}$, Eqs.(2.36) and (2.37), for the case of 3 qubits. The matrix product of the three controlled gates gives a result a matrix $2^3 \times 2^3$ where the 00 element is 1 and the other elements of the first row and first column are zero. The elements of the remaining columns and rows are a combination of zeros and random values. By computing several times the configuration shown in the left side of the figure, the resulting gate is the searched Haar gate.*

For the case of $n = 3$ qubits, we will have the setup described in Fig.2.10. And, in general, for n qubits, the setup to compute the Haar gates, Eqs.(2.36) and (2.37), is built using n controlled gates ($C_0 - W$, $C_1 - W$,..., $C_{n-1} - W$), where the control qubit is different on each gate and all the qubits end up being a control qubit.

2.3.2 Considerations on the hypothesis test

Following the same procedure that the one described in the previous protocols, we need to carry out a hypothesis test to know the number of measurement, N, required to estimate the expectation value of $\langle \phi^- | \rho_A \otimes \rho_B | \phi^- \rangle$. Picturing the worst case scenario where Bob wants to fool Alice seems a harder task that in the case of the previous protocols, sections 2.1.1 and 2.2.1. The reason of that is that in this case, using Haar gates, the values used are completely random, implying that the chances that Bob generates an eigenstate orthogonal to $|\gamma_0\rangle$ are really low. Therefore, like in the case of using Z_ϕ gates, we can guess that the number of different circuits configurations required to know if Bob has generated also $|\gamma_0\rangle$ with a small probability of being wrong is $k' < k$, being k the expression shown in Eq.(2.25).

The number of experimental runs needed to estimate the expectation value of the Bell measurements up to a given precision and a given probability in each of the different circuit configurations, is the same that in the previous protocols, n_e. Eq.(2.31). So, the total number of measurements is, $N = k' \times n_e$.

Finally, the advantage of the last two protocols explained in this chapter (using Haar gates or Z_ϕ gates with random phase as controlled gates on Alice's and Bob's circuit), is clear when taking about the number of different cirucit configuration needed to carry out the protocol. Comparing now the protocols of Z_ϕ gates and Haar gates, even though it is a bit easier for Bob to manipulate Alice when using random phases, constructing Haar gates is not an easy task, as it was shown in section 2.3.1.

Chapter 3

Conclusions and outlook

In this thesis we have shown three different cross-platform verification protocols, where the goal is to compare two quantum states generated by two different quantum devices, Alice's and Bob's quantum circuits. Specifically, they check if Bob has generated the same state as Alice, $|\gamma_0\rangle$, Eq.(1.8).

The first protocol presented uses a controlled-unitary constructed by applying a Z gate on a different qubit of the system in each circuit configuration computed. In the next protocol, a different phase is also applied between the different eigenstates, but in this case the controlled-unitary is formed by n Z_ϕ gates with different random phases on the different qubits leading to a unitary where all eigenstates have different eigenvalues. So, just one circuit configuration is needed in the latter. The last protocol showed uses a special construction of Haar gates, where $|\gamma_0\rangle$ eigenvalue is 1 and the rest of the states $|\gamma_j\rangle$ are random values. Finally, we also study how the different protocols scale with the system size.

What we present in this project is just a first building block in the very ambitious program of scaling up quantum devices with a new architecture, demanding novel algorithms and tools. The most basic one considered here is to compare two states. The last comparison reminds of file verification [18], to check if one file (quantum state) is the same as a previous one, the "desired" one.

3.1 Quantum hashing and quantum fingerprints

In this chapter, we will introduce the cryptographic hash functions [21] and the fingerprint algorithm [22], [23], and show that the comparison between two hash functions or two fingerprints is how the security protocol of data verification works.

A cryptographic hash function is a mathematical function that maps data of arbitrary size to a short, fixed-length, hash value with some properties. One of the tasks of these functions is to resist different cryptanalytic attacks. To do so, they are defined following three specific properties: pre-image resistance, second pre-image resistance and collision resistance.

The first one implies that hash functions are one-way functions, meaning that it is too difficult to find their pre-image. In other words, given a hash value h, it is hard to find a message, m, such that $h = hash(m)$. On the other hand, given a message m, it is easy to compute a hash value that $h = hash(m)$.

The second property, the second pre-image resistance, shows that given an input message m, it should be difficult to find another message, m', such that $m \neq m'$ and $hash(m) = hash(m')$.

The last property is like the “strong" version of the previous one. It says that it should be difficult to find two different messages, m and m', such that $hash(m) = hash(m')$.

The set of these properties imply that a small change in a message produces such a change in the hash value that a new one is generated (avalanche effect)[21]. Consequently, an adversary can not change the input data without changing the hash function.

Therefore, cryptographic hash functions can be used in file verification. In order to make sure that a file has not been modified, hash-based protocols compare the file's hash value to a previously calculated one. If the values match, we can suppose that the file has not been corrupted.

Fingerprints, analogously to hash functions, are mathematical functions that map a great amount of data to a smaller string, its fingerprint (like human fingerprints). However, fingerprints do not need to follow the three properties aforementioned for hash functions. The condition that they must meet is that its probability of collision, i.e. two files of data having the same fingerprint, has to be negligible. There are several ways of computing them, and one is using cryptographic hash functions. Fingerprints are usually used to avoid the comparison and transmission of big blocks of data. For example, in file verification, a web browser can check if a remote file has been corrupted by comparing its fingerprint with the one of the previous copy [24].

Hash functions and fingerprints have their quantum representation [22], [25]. Buhrman et.al. [22] propose to use a SWAP test to compare if the fingerprints of Alice and Bob, $|\phi_A\rangle$ and $|\phi_B\rangle$, are the same. As it was already mentioned in chapter 1, to carry out a SWAP test implies teleporting the states for their comparison through a quantum link. However, a quantum link teleporting large quantum states between two different devices is not currently accessible.

Therefore, to compare the different hash functions, $|h_A\rangle$ and $|h_B\rangle$, or the different fingerprints, $|\phi_A\rangle$ and $|\phi_B\rangle$, we can use any of the algorithms explained in chapter 2.

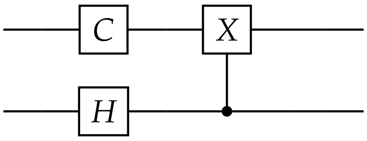


Figure 3.1: *Alice and Bob circuits used for file verification with hash functions and fingerprints. C represents the quantum circuits that generates the quantum hash functions and the quantum fingerprints and $C - X$ the different controlled-gates in the C basis of the protocols previously shown in chapter 2.*

Fig.3.1 shows Alice's and Bob's circuits and how they would be used for quantum data verification. Gate C represents the quantum algorithm that generates the quantum hashing functions or the quantum fingerprints, and $C - X$ the controlled unitaries of the different protocols in the C basis. Recalling that we are working under the assumption that we trust that Alice generates the searched state $|\psi_0\rangle$ and that we check if Bob has generated the same, we can make some analogies with the case of file verification. The state that Alice generates can be interpreted as the quantum hashing function or the quantum fingerprint of the original quantum data, i.e. the quantum data that is known to be unmodified, and Bob generates the hash value of the quantum data that is checked whether it has been changed. The comparison is made by carrying out Bell measurements of the ancilla qubits.

In conclusion, besides being useful in quantum distributed computation, the latter protocols may be also find used in security protocols.

3.2 Comparison with the state-of-the-art.

Additionally, the latter protocols present some advantages compared to the state-of-the-art, [7]. The latter, uses quantum tomography to compute the fidelity, Eq.(1.2), of the output states ρ_1 and ρ_2. Quantum tomography implies the measurement of the states and their consequent destruction (due to the collapse of the wavefunction) if the measurements are incompatible. Therefore, every time an incompatible measurement of the output is carried out, the states need to be constructed again. On top of that, the scaling of the experimental tests with the system size, 2^{bn}, makes it unsuitable for large systems [7].

On the other hand, in the protocols we explain here, chapter 2, we measure the ancilla of the circuits, implying that there is no need to generate the output states after every measurement, as long as the tensor product structure system-ancilla is preserved. Regarding the scaling, in the protocol where the unitaries are computed by Z gates, the number of different circuit configurations needed goes with the number of qubits of the generated states, Eq.(2.25). This dependence can be logarithmic if $\delta' = 1/poly(n)$. Additionally, in the protocols where the unitaries are Haar gates and Z_ϕ gates with random phase, we can guess, due to the randomness of the eigenvalues of the eigenstates orthogonal to the searched state, that the number of different circuit configurations needed is $k' < k$. On top of that, in the three protocols shown in this project, the number of experimental test required goes with the precision we want in the estimation of $\langle \phi^- | \rho_A \otimes \rho_b | \phi^- \rangle$, ε.

Finally, regarding the state-of-the-art, Elben et.al. [9] show that for a 10-qubit system, the number of measurements needed to compute an estimation of the fidelity [*] for an statistical error of $\varepsilon = 0.05$ is of the order of $10^4 - 10^5$. Moreover, for the protocols of this project, setting $\varepsilon = \delta' = \delta'' = 0.05$ we obtain $n_e = 738$ and $k = \lceil 4.30 \rceil = 5$. Therefore, the number of measurements required for the Z-gate protocol, section2.1, is $N = kn_e \approx 4000$, of the order of 10^3, and for the last two protocols explained in chapter 2, $N = k'n_e < 4000$. This indicates that better results than the ones that the state-of-the-art shows may be achievable.

[*] $|F_{max}(\rho_1, \rho_2)_e - F_{max}(\rho_1, \rho_2) \leq \varepsilon|$, where $F_{max}(\rho_1, \rho_2)$ is the target fidelity and $F_{max}(\rho_1, \rho_2)_e$ is the estimated one

Acknowledgements

I could not finish this research project without mentioning my supervisor **Dr.Jordi Tura i Brugués**. Mostly, I want to highlight his continuous supervision from the start to the end of this project (sometimes even on weekends). This work was accomplishes due to his interest and wise feedback and help for every result carried out.

I would also like to offer my profound thanks to the PhD student **Stefano Polla** for his invaluable help in the simulations done to check some of the results shown in this project.

During the project, I appreciated uncountable times the background gained from the splendid *Applied Quantum Algorithms* lectures given by **Dr.Vedran Dunjko** and **Dr.Jordi Tura i Brugués**.

I am really thankful to **Dr.Vedran Dunjko** for the consideration of my request to be a second corrector.

Finally, my special thanks go to my family and friends, in Leiden and Spain, for their extra support that helped me to present this work.

Bibliography

[1] R. P. Feynman, “Simulating physics with computers,” *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467–488, 1982.

[2] F. Arute *et al.*, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, pp. 505–510, 7779 Oct. 2019. DOI: 10.1038/s41586-019-1666-5.

[3] J. Preskill, “Quantum Computing in the NISQ era and beyond,” *Quantum*, vol. 2, p. 79, Aug. 2018. DOI: 10.22331/q-2018-08-06-79. [Online]. Available: https://doi.org/10.22331/q-2018-08-06-79.

[4] ——, *Quantum computing 40 years later*, 2021. arXiv: 2106.10522 [quant-ph].

[5] T. Häner, D. S. Steiger, T. Hoefler, and M. Troyer, “Distributed quantum computing with qmpi,” May 2021. [Online]. Available: http://arxiv.org/abs/2105.01109.

[6] R. Jozsa, “Fidelity for mixed quantum states,” *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994. DOI: 10.1080/09500349414552171. eprint: https://doi.org/10.1080/09500349414552171. [Online]. Available: https://doi.org/10.1080/09500349414552171.

[7] J. Carrasco, A. Elben, C. Kokail, B. Kraus, and P. Zoller, “Theoretical and experimental perspectives of quantum verification,” *PRX Quantum*, vol. 2, 1 Mar. 2021. DOI: 10.1103/prxquantum.2.010102.

[8] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, “Quantum state tomography via compressed sensing,” *Phys. Rev. Lett.*, vol. 105, p. 150 401, 15 Oct. 2010. DOI: 10.1103/PhysRevLett.105.150401. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.105.150401.

[9] A. Elben *et al.*, “Cross-platform verification of intermediate scale quantum devices,” *Phys. Rev. Lett.*, vol. 124, p. 010 504, 1 Jan. 2020. DOI: 10.1103/PhysRevLett.124.010504. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.124.010504.

[10] A. Haar, “Der massbegriff in der theorie der kontinuierlichen gruppen,” *Annals of Mathematics*, vol. 34, no. 1, pp. 147–169, 1933. [Online]. Available: http://www.jstor.org/stable/1968346.

[11] D. Gross, K. Audenaert, and J. Eisert, “Evenly distributed unitaries: On the structure of unitary designs,” *Journal of Mathematical Physics*, vol. 48, no. 5, p. 052 104, 2007. DOI: 10.1063/1.2716992. eprint: https://doi.org/10.1063/1.2716992. [Online]. Available: https://doi.org/10.1063/1.2716992.

[12] C. Dankert, R. Cleve, J. Emerson, and E. Livine, "Exact and approximate unitary 2-designs and their application to fidelity estimation," *Phys. Rev. A*, vol. 80, p. 012 304, 1 Jul. 2009. DOI: 10.1103/PhysRevA.80.012304. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.80.012304.

[13] R. W. Hamming, "Error detecting and error correcting codes," *The Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950. DOI: 10.1002/j.1538-7305.1950.tb00463.x.

[14] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ser. STOC '96, Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. DOI: 10.1145/237814.237866. [Online]. Available: https://doi.org/10.1145/237814.237866.

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

[16] V. V. Shende and I. L. Markov, *On the cnot-cost of toffoli gates*, 2008. arXiv: 0803.2316 [quant-ph].

[17] A. Barenco *et al.*, "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, pp. 3457–3467, 5 Nov. 1995. DOI: 10.1103/PhysRevA.52.3457. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.52.3457.

[18] D. Armstrong, "Global information assurance certification paper an introduction to file integrity checking on unix systems with an example deployment using the no-cost samhain file integrity checker," 2003.

[19] M. Dekking, *A modern introduction to probability and statistics : understanding why and how*. Springer, 2005, pp. 45–46.

[20] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963. DOI: 10.1080/01621459.1963.10500830. eprint: https://www.tandfonline.com/doi/pdf/10.1080/01621459.1963.10500830. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/01621459.1963.10500830.

[21] S. Al-Kuwari, J. H. Davenport, and R. J. Bradford, *Cryptographic hash functions: Recent design trends and security notions*, Cryptology ePrint Archive, Report 2011/565, https://eprint.iacr.org/2011/565, 2011.

[22] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," *Physical Review Letters*, vol. 87, no. 16, Sep. 2001. DOI: 10.1103/physrevlett.87.167902. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.87.167902.

[23] M. Rabin, *Fingerprinting by Random Polynomials*, ser. Center for Research in Computing Technology: Center for Research in Computing Technology. Center for Research in Computing Techn., Aiken Computation Laboratory, Univ., 1981. [Online]. Available: https://books.google.nl/books?id=Emu%5C_tgAACAAJ.

[24] A. Broder, "On the resemblance and containment of documents," in *Proceedings. Compression and Complexity of SEQUENCES 1997 (Cat. No.97TB100171)*, 1997, pp. 21–29. DOI: 10.1109/SEQUEN.1997.666900.

[25] F. Ablayev and A. Vasiliev, *Quantum hashing*, 2013. arXiv: 1310.4922 [quant-ph].