Noise robustness of a multiparty quantum summation protocol

Antón Rodríguez-Otero, Niels M. P. Neumann, Ward van der Schoot, and Robert Wezeman

The Netherlands Organisation for Applied Scientific Research, The Netherlands, The Hague

Abstract. Connecting quantum computers to a quantum network opens a wide array of new applications, such as securely performing computations on distributed data sets. Near-term quantum networks are noisy, however, and hence correctness and security of protocols are not guaranteed. To study the impact of noise, we consider a multiparty summation protocol with imperfect shared entangled states. We study analytically the impact of both depolarising and dephasing noise on this protocol and the noise patterns arising in the probability distributions. We conclude by eliminating the need for a trusted third party in the protocol using Shamir's secret sharing.

Keywords: Distributed Quantum Computing · Noisy Quantum Communication · Multi-Party Computation · Shamir Secret Sharing

1 Introduction

Quantum computing is an emerging field where advances are made on the hardware-side, software-side, as well as applications. Many companies and universities are working on building better quantum hardware with more resources of better quality. At the same time, new algorithms are being discovered, and these new quantum algorithms are applied in various new settings.

The theoretical speedup quantum computers offer for various problems discerns them from classical alternatives. Amongst these are some of the most complicated problems encountered in every-day life. Examples where quantum computers outperform classical alternatives include breaking certain asymmetric encryption protocols [21], developing new materials and personalised medicines [10], and solving complex systems of linear equations [12].

Another aspect at which quantum computers distinguish themselves from classical alternatives, is the security of a quantum state: Opposed to classical information, in general, quantum information cannot be read out or copied faithfully. Reading out a quantum state destroys the state irrevocably and loses information, whereas trying to copy a quantum state leaves the state and its copy entangled, and operations performed on an entangled copy differ from those applied to the original unentangled state. Because of this, sharing information via

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

quantum states is secure. This idea underlies the field of quantum communication and its subfield quantum key distribution.

Combining quantum computing with quantum communication joins the best of both worlds: by using quantum communication between different quantum computers, these devices can collaboratively solve larger problems, while the information shared between the devices remains secure. This field is called *Distributed Quantum Computing* (DQC).

Distributed quantum computing entails the collaborative execution of quantum algorithms using multiple quantum devices. Distributed computations can occur at various levels: for example, the devices may independently run their own quantum circuits, after which the outputs are combined to obtain the final results. Alternatively, the devices may cooperate intricately through quantum communication to execute a single overall circuit. This study concentrates on the latter scenario, specifically exploring the execution of a distributed quantum addition circuit.

The key challenge in this form of distributed quantum computing, is the application of non-local multi-qubit gates. As any multi-qubit gate can be decomposed into CNOT gates with additional local one-qubit gates [3], it suffices to implement the CNOT-gates in a non-local fashion. Eisert et al. gave the first description of how to perform operations between different quantum devices through the use of local operations and classical communications (LOCC) and shared entanglement between the different devices [9]. Later, this work was extended and a distributed version of Shor's algorithm was theorised [25,24].

Distributed quantum computing works by transforming traditional quantum algorithms to their distributed version. In these distributed versions, operations performed between qubits located on different devices are called non-local and are replaced by a non-local quantum gate established using shared entangled states. In comparison, operations between qubits on the same device are called local, and are unchanged. These three works consider all operations, both local and non-local, to be perfect. Beals et al. later proved that distributing an algorithm over different resources incurs only a small overhead in the cost [4]. Hence, when programming quantum algorithms on a higher level, the underlying structure of the hardware, local or distributed, has only a marginal effect.

Follow-up work mainly focused on applications run using a distributed quantum network [7], or on how to best implement a distributed quantum computer network [11,5]. One aspect to take into account in these distributed networks is the robustness against noise, as current hardware is noisy and will remain so for the foreseeable future. It is therefore interesting to consider the effect of imperfect operations in such distributed settings. A first work on this topic computed the fidelity of a distributed and imperfect quantum phase estimation algorithm, when distributed over a varying number of devices [16]. Another example is the work by Khabiboulline et al. where a secure quantum voting protocol is presented [14].

In this work, we extend this line of research by considering imperfect non-local operations as well, but applied to the distributed quantum summation

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

protocol [17], which extends the algorithm proposed by Draper [8] and later improved by Ruiz-Perez and Garcia-Escartin [19]. The quantum summation algorithm uses the Quantum Fourier Transform to map the states to their phase state representation. In the phase space, addition corresponds to specific controlled phase gates.

In this protocol, we consider different parties which aim to compute the sum of their inputs, without revealing these inputs. Each party has access to a local quantum computer, which can generate shared entangled states with other devices. In practice, quantum hardware remains noisy and it is necessary to consider decoherence effects when developing applications. Currently, the fidelity of state teleportation between non neighbouring nodes is around 0.7 [13] while the fidelity of quantum operations on quantum devices is around 0.95 to 0.99 [15]. For this reason, we omit in this work the effect of imperfect quantum operations, and focus on the impact of an imperfect quantum network links. Concretely, we consider how dephasing and depolarising noise on the shared entangled states affects the output fidelity of this distributed summation protocol.

We also extend this line of research by combining it with a primitive from cryptography called *Shamir Secret Sharing*. In earlier works, multiparty protocols are considered with the use of a central server party which is trusted by everyone. This is not a realistic assumption in practical use cases. In this work, we show how the considered multiparty summation protocol can be extended to a setting without the requirement of a trusted server party. We show that the protocol yields the same output as the original protocol, while none of the parties learns inputs from other parties.

Section 2 explains the multiparty summation protocol and the two considered noise models. Next, Section 3 presents the results of simulations for both noise models. Section 4 contains an analytical study of the noise patterns and the periodicity therein. Afterwards, Section 5 details the extension of the protocol to a version without the need of a trusted server party. Section 6 concludes with a summary and an outlook to future distributed quantum computing work.

2 Preliminaries

2.1 Distributed Quantum Computing

We start by describing the non-distributed version of the quantum summation protocol, after which we explain the distributed version from [17]. Suppose we have two integers $a, b < 2^n$ that we wish to add and that we have their corresponding quantum states $|a\rangle$ and $|b\rangle$ that are their binary representation using n qubits. The protocol first applies the quantum Fourier transform of size n, denoted by QFT_n to $|b\rangle$. This yields the phase state representation of b, given by $|\phi(b)\rangle$. Then, applying phase gates to the qubits of $|\phi(b)\rangle$ controlled by the qubits of $|a\rangle$ gives the quantum state $|\phi(a+b)\rangle$. After applying an inverse quantum Fourier transform, the state $|a+b\rangle$, describing the binary representation of $a+b$, is obtained.

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

This summation protocol can be easily extended to allow a server party to do the addition of k different numbers held by k different computing parties. Figure 1 showcases the extended protocol for two computing parties with an additional server party. The server party holds the result at the end of the protocol. Note that the phase gates applied by different parties commute and hence, every party can apply their local phase gates simultaneously.

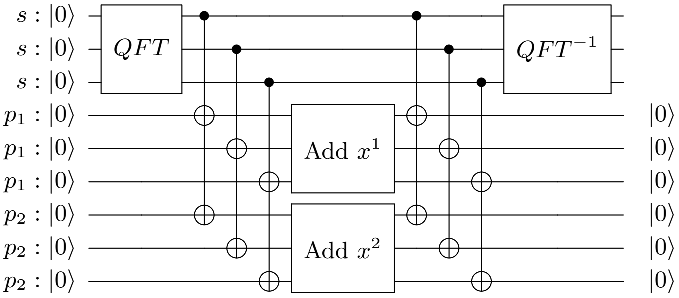


Fig. 1. Example of **DQA** [17]. A server party adds integers from two computing parties. The blocks Add x^k denote the phase-gates needed to add integer x^k as described above. The final quantum state in the first register is $|x^1 + x^2\rangle$.

The above multiparty protocol translates to a non-local protocol by replacing every CNOT gate by a non-local CNOT gate. The resulting protocol is called the *DISTRIBUTED-QFT-ADDER* (**DQA**). Multiple implementations for the CNOT-gates exist, some of which even allow simultaneous implementation of the phase gates by all parties [17].

2.2 Noise models

The quantum network distributes entangled GHZ states between the server node and the different party nodes. The presence of noise translates to imperfect entanglement between the nodes.

Current state-of-the-art protocols for entanglement generation between nodes of a quantum network are heralded, which allows to deterministically know whether the entanglement distribution process succeeded. Typically, heralding work in experiments via a photon measurement such that entanglement is established if and only if a photon has been detected. We therefore disregard lossy quantum channels by assuming that the distribution is done in a heralded way.

In this study, we consider two types of noise in the quantum links, namely dephasing and depolarising noise. These types of noise arise often in physical implementations and current software packages allow for easy simulation of these noise type, whilst the analytic study remains feasible at the same time. The respective noise channels are applied to the quantum links by applying them to all qubits in the GHZ state independently.

Noise model A: Dephasing channel A dephasing channel is a *completely positive and trace-preserving* (CPTP) map that represents the decay of the quantum phase of a system, that is, the off-diagonal elements of the density matrix. A one-qubit dephasing channel ε_{depha} is usually represented by the map

$$\varepsilon_{depha} : \rho \mapsto \left(1 - \frac{p}{2}\right)\rho + \frac{p}{2}\mathbf{Z}\rho\mathbf{Z} \tag{1}$$

which performs a phase flip with probability $p/2$. Writing the matrix representation of this channel we see, indeed, that it corresponds to a phase damping process:

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \to \varepsilon_{depha}(\rho) = \begin{pmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{pmatrix}. \tag{2}$$

Dephasing errors arise in fiber optic links due to the birefringence phenomenon, which is associated with changes in the refractive index for different polarisations or different regions of the material [22]. In fact, using a special polarisation maintaining optical fiber, the decoherence in these links can be completely described via dephasing processes [23]. Assuming heralded entanglement distribution, we can ignore the high attenuation arising in these links. Our focus is the impact of noise on the fidelity of the protocol, so we omit the entanglement generation rate and the lower transmission rates.

Noise model B: Depolarising channel The depolarising channel is usually seen as the quantum equivalent of white noise. Depolarising channels model processes that completely scramble the starting state with some probability. As a result, both quantum and classical information is lost. Given a valid n-qubit quantum state ρ, an n-qubit depolarising channel ε_{depol} can be written as

$$\varepsilon_{depol} : \rho \mapsto (1-p)\rho + \frac{p}{d}\mathbf{I}, \tag{3}$$

where $d = 2^n$ is the dimension of the Hilbert space ρ lives in.

Depolarising channels can, amongst other things, model the misalignment of reference frames between the nodes in a quantum network [26]. Moreover, depolarising channels can also model what happens if heralding fails, for instance when the detector wrongfully measures a photon. Such an event is called a dark count and leads to reading out an empty quantum memory [6].

3 Simulations with noise

We simulated the quantum summation protocol **DQA** [17] and included the noise models discussed above to see how well the protocols perform in noisy settings. By adding dephasing or depolarising noise to the protocol, we expect incorrect outcomes found by the server party at the end of the protocol. Therefore, we report the results as probability distributions in histograms or polar plots.

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

We implemented both noise models using Qiskit [1] where we applied the noise models only to the quantum links, the part where the GHZ-states are generated. We implemented these noise models by inserting local noisy identity gates at the end of the GHZ generation block. We ran experiments for varying number of parties and inputs, as well as noise levels. Each simulation consists of 9,000 independent runs of the circuit[1].

3.1 Dephasing noise

We first consider the impact of the dephasing noise by analysing four parties, each with input 1 and a dephasing noise of $p/2 = 0.07$ for each of the four quantum links.

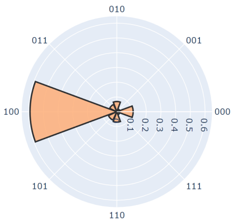
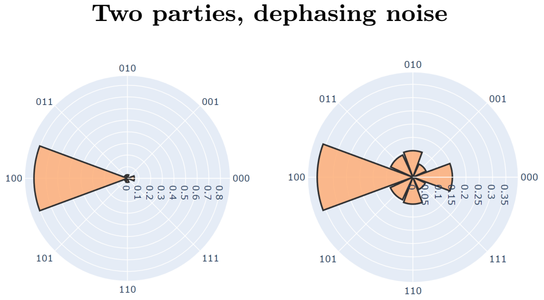


Fig. 2. Polar representation of the distribution .


Two parties, dephasing noise

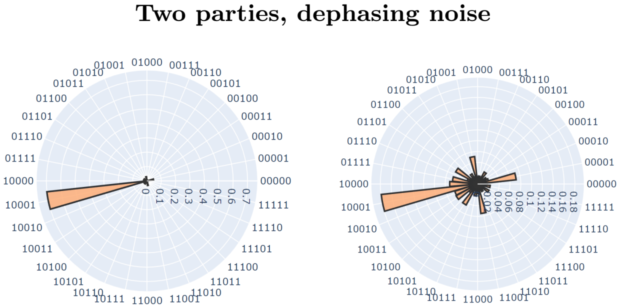
(a) $p/2 = 0.05$

(b) $p/2 = 0.25$

Fig. 3. Probability distribution for the case of two parties inputting 2, with identical dephasing noise applied on each entangled qubit pair for varying noise levels, $p/2$, as indicated. The correct outcome is given by 100 in binary.

[1] The implementations are available upon reasonable request to the authors.

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26



(a) $p/2 = 0.05$ (b) $p/2 = 0.25$

Fig. 4. Probability distribution for the case of two parties with inputs 10 and 7, respectively, with identical dephasing noise applied on each entangled qubit pair for varying noise levels, $p/2$, as indicated. The correct outcome is given by 10001 in binary.

In the noisy setting, the correct outcome, 4 or 100 in binary, has the highest probability, followed by outcome 000. The probability distribution seems to have some symmetry (cf. Section 4), hence Figure 2 shows the probability distribution in a polar plot. The second most frequent outcome is diametrically opposed to the correct one; and the next two most frequent outcomes are $\pi/2$ radians away from the highest probability and diametrically opposed to each other.

Interestingly, this symmetry emerges also for a different number of parties and for varying inputs. First, Figure 3 shows the results for a protocol run with two parties, both of them inputting 2, for varying values of p. Again, a similar noise pattern emerges, indicating that the noise pattern is independent of the number of parties involved. Finally, Figure 4 shows the results for a protocol run with two parties, where one of them inputs 10 and the other 7, again for varying values of p. We again see similar symmetries appearing in the noise probability distribution, which indicates that the probability distribution is independent of the input values of the parties.

3.2 Depolarising noise

We also performed the analysis for depolarising noise instead of dephasing noise. Interestingly, the same probability distributions were found as for dephasing noise, with the same symmetry patterns emerging. We hence omitted the figures, as they give no additional information compared to the figures in the previous circuit. In the next section, we proof that indeed the probability distributions follow a specific pattern with symmetries, independent of the type of noise.

4 Analytical study

The probability distributions shown in the previous sections show some symmetry. In this section we analyse this symmetry effect and show that, for fixed

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

error probability, indeed the weighted Hamming distance with the correct output string determines the probability of being measured. We derive an expression for the probability distribution that applies to both dephasing and depolarising noise, and then discuss the intuition on the relation between the analytical expression and the observed pattern. Proofs of the results presented in this section can be found in Appendix A and in the full version of this paper [18].

4.1 Proof of probability distribution

The probability distribution of the **DQA** under dephasing or depolarising noise follows a specific probability distribution.

Lemma 1. *Under depolarising or dephasing noise, the server party state right before the application of the Inverse Quantum Fourier Tranform on a **DQA** for n parties can be written as*

$$\rho = \bigotimes_{s=0}^{n-1} \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + ae^{-i\theta_s}|0\rangle\langle 1| + ae^{i\theta_s}|1\rangle\langle 0|), \tag{4}$$

where $a = \prod_{i=0}^{n-1} a_i$, with $a_i = (1-p_i)^2$ for dephasing noise and $a_i = 1-(1-p_i)^2$ for depolarising noise, with p_i the noise parameter for party i.

Now, to characterise the output probability distribution of the distributed adder protocol, we need to look at the product of the a_i factors. As we consider the same error rates for every qubit, we define the fidelity parameter a as $a = \prod_{i=0}^{n-1} a_i$. In particular, $a = 1$ corresponds to a noiseless GHZ-state, whereas $a = 0$ corresponds to a completely dephased or depolarised GHZ state.

Theorem 1. *Let $\{t^{(i)}\}_{i=1}^{m}$ be the inputs of m different parties and let for each $s \in \{0, 1, \ldots n-1\}$*

$$\theta_s = \frac{\pi}{2^{n-1-s}} \sum_{i=1}^{m} t^{(i)} = \frac{2\pi}{2^{n-s}} \sum_{i=1}^{m} t^{(i)}. \tag{5}$$

*Then, the m-player **DQA** protocol produces the output probability distribution such that for each potential output x*

$$P(x) = \frac{1}{2^n} \prod_{s=0}^{n-1} [1 + a\cos(\theta_s - 2\pi x/2^{n-s})], \tag{6}$$

with fidelity parameter $a \in [0, 1]$ related to the depolarising or dephasing noise level.

4.2 Understanding the noisy distribution

This section provides intuition for what the proven theoretical distribution in Equation (6) actually looks like and how it translates to the distribution observed in the simulations. From the equation, it follows that the probability is

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

maximised if all cosines evaluate to 1, which happens precisely if the argument of the cosines is an integer multiple of 2π. Setting $x = \tilde{x}$, with $\tilde{x}$ the correct outcome of the summation, this indeed maximises the probability. The resulting probability then equals

$$P(\tilde{x}) = \left(\frac{1+a}{2}\right)^n .$$

A noiseless setting where $a = 1$, indeed gives a probability of 1.

Now, if $y \in \mathbb{Z}_{2^n}$ is a different outcome, y can be written as $y = \tilde{x} + z$ for some error $z \in \mathbb{Z}_{2^n} \backslash \{0\}$. The probability to observe y then equals

$$P(y) = \frac{1}{2^n} \prod_{s=1}^{n} [1 + a\cos(2\pi z/2^s)] \tag{7}$$

Note, we relabeled the counter with respect to Equation (17). For every s, we see a periodic behavior in z resulting from the cosines. Combined, we get a complex periodic behavior in the probability distribution of the possible outcomes.

We can now prove that the probability distribution is symmetric around x:

Lemma 2. *Let $z \leq 2^{n-1}$, then $P(x + z) = P(x + (2^n - z))$.*

By the previous lemma, information on noise strings $z \leq 2^{n-1}$ gives sufficient information on all possible noise strings.

In addition, this allows us to show the behaviour observed in Section 3 regarding the second and third most frequent outcomes:

Lemma 3. *For any integer $k \in \{1, \ldots, n-1\}$ and any error string $z \in \{1, 2, \ldots 2^k\}$, we have that*

$$P(x + 2^k) \geq P(x + z)$$

This lemma yields indeed that the state diametrically opposite to the correct outcome has the second largest probability, the states $\pi/2$ radians away from the correct outcome have the third largest outcome, and so forth.

In addition, we see that the probabilities closer to the correct value are larger. To be more precise:

Lemma 4. *For any integer $k \in \{1, 2, \ldots, n-1\}$ and error string $z \in \{1, 2, \ldots, 2^k\}$, we have*

$$P(x + z) \geq P(x + (2^{k+1} - z))$$

Running the circuit multiple times gives samples from the probability distribution. It would be natural to try and use multiple circuit runs to increase the probability of obtaining the correct answer, for example by comparing the obtained distribution with the theoretical distribution derived above. However, as for fixed fidelity parameter a the probabilities are exponentially small in n, standard techniques using Chernoff bounds require an exponential number of samples to lower bound the success probability of retrieving x.

5 Protocol without Trusted Server

Like most multiparty protocols, the **DQA** protocol requires a trusted third party. Although this is a common assumption in some classical multiparty computation protocols, it is unrealistic in practice. This section therefore introduces a modification to the protocol which eliminates the necessity of this reliable authority.

For this modification to work, a certain primitive from cryptography is required, called *(Treshold) Shamir's Secret Sharing* [20] (SSS), a well-known classical protocol originally intended to distribute secrets between several entities, with the ability to reconstruct them.

Suppose an agent desires to distribute a secret X among k parties. Then the agent would choose a polynomial of order $t < k$ over a finite field $GF(q)$

$$g(x) = X + a_1 x + \ldots + a_{t-1} x^{t-1} \tag{8}$$

with a prime number q such that $X < q$. Next, the secret sharer would choose a set of k different points $\{x_1, \ldots, x_k\}$ to evaluate the polynomial on and would send one polynomial evaluation $g(x_j)$ to each party. Now, any subset of t parties can reconstruct the secret by simply performing polynomial interpolation using the polynomial evaluations that they received and then determining $g(0) = X$. Interpolation requires t parties, as the polynomial has degree $t-1$. Knowing $t-1$ shares $\{(x_i, g(x_i))\}$ does not provide any information about the secret.

SSS can be utilized to perform multiparty summation in a secure manner by combining it with repeated usage of **DQA** in multiple rounds. In each round, a different party acts as server of **DQA**, the other parties input one of their shares for the quantum protocol. The party acting as server then receives the sum of the shares at the end of the round. As shares are only used as input in the quantum protocol, no party learns the shares of other parties By combining the shares of any subset of at least t parties, the parties can reconstruct the summation result. This results in the following protocol:

NO-TP-ADDER (NTPA)

Consider m parties, each holding a number X_i.

- **Step 1:** the parties agree on a sufficiently large prime q and make q public;
- **Step 2:** each party i chooses a degree-t polynomial over the finite field $GF(q)$

  $$g_i(x) = X_i + a_1^i x + \ldots + a_{t-1}^i x^{t-1} \tag{9}$$

  where the coefficients are chosen at random but non-zero, except for a_0^i, which corresponds to the real input from the party ($a_0^i = X_i$);
- **Step 3:** In each round, a different party will act as the server party, which requires agreement on the order for the parties to act as server;
- **Step 4:** m rounds of **DQA** are performed. For each $r \in \{1, \ldots, m\}$:
  - Party r acts as server;
  - Party i inputs share $g_i(r)$;
  - Party r receives the partial summation $\sum_i g_i(r)$

  At the end of all rounds, each party r has received the partial summation $\sum_i g_i(r)$. It hence knows $G(r)$ for $G(x) = \sum_{i=1}^m g_i(x)$

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

– **Step 5:** The summation result can be restored by having t parties cooperate to share their intermediate results $G(r)$. As $G(x)$ has degree at most $t-1$, these t evaluation points of $G(x)$ are hence sufficient to reconstruct $G(x)$, from which the summation result can be computed by evaluating $G(0) = \sum_{i=1}^{m} g_i(0) = \sum_{i=1}^{m} X_i$. Note that just like in the original SSS protocol, at most $t-1$ shares are not sufficient to conclude anything about $\sum_{i=1}^{m} X_i$.

As each party acts as a server once, no party holds more power or knowledge than any other, eliminating the need for a trusted third party.

Note that as the parties only know the intermediate shares $G(r)$, they still need t shares to recover the result of the summation.

6 Conclusions and outlook

As current quantum hardware is noisy, and is expected to remain so for a while, it is important to study the impact that imperfect operations have on the fidelity of quantum protocols. Multiple works on noisy quantum algorithms are available in literature. Similarly, a few works on distributed quantum computing are available. This work focuses on the combination of distributed noisy operations and analyses the effect of imperfect operations on the outcome. We restricted ourselves to imperfect shared entangled states with perfect operations on the individual devices, as the errors within local devices are generally smaller than the ones seen on quantum communication.

We considered a practical implementation of the distributed multiparty quantum summation protocol [17]. We apply depolarising or dephasing noise on the shared entangled states and analytically study the behaviour of the protocol. The probability distributions corresponding to the final state of a noisy summation protocol given these noise models show a clear symmetric pattern, proved in the analytic study. The probability to find an erroneous state depends on the amount of noise affecting the execution of the protocol and the weighted Hamming distance between the erroneous string and the correct outcome.

The protocol initially uses a trusted third party. Building upon the classical Shamir's Secret Sharing protocol, we could remove the need for a trusted party. As an added benefit, all parties automatically learn the outcome of the protocol.

Future work should address the effects of other sources of noise that are present in the protocol, such as imperfect local operations. More importantly, a proper study of the effects that noise has on the security of the protocol needs to be done. In a perfect noiseless setting, the quantum no-cloning theorem ensures that no information is leaked to the outside world without corrupting the states that the parties share; thus, the parties could detect the presence of an adversary and abort the protocol before inputting their secrets. However, the signature on the shared entangled states of the action of an eavesdropper is indistinguishable from noise. Hence, the parties cannot expose an eavesdropper just by checking quantum correlations via the shared entangled states. In this case, the amount of information that can be leaked and learned by an eavesdropper from the execution of the protocol should be bounded. As a first step, formal definitions of

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

security, anonymity and privacy in the context of quantum multiparty summation must be established, similar to the field of Quantum Electronic Voting [2].

Although the conclusions from the present study are specific for the investigated protocol, most quantum multiparty protocols rely on the utilisation of entanglement at some stage. Thus, the methodology used here can inspire the analysis of noise robustness in similar protocols.

A Proofs of Results of Section 4

Lemma 5. *Under depolarising or dephasing noise, the state of the server party right before the application of the Inverse Quantum Fourier Tranform on a* ***DQA*** *run for n parties can be written as in 4; where $a = \prod_{i=0}^{n-1}(1-p_i)^2$ for dephasing noise and $a = \prod_{i=0}^{n-1}[1-(1-p_i)^2]$ for depolarising noise, with p_i the noise parameter for party i.*

Proof. From the effect that a one qubit *dephasing channel* has on an n-qubit GHZ state

$$\begin{aligned}\rho &\mapsto \left(1-\frac{p_i}{2}\right)\rho + \frac{p_i}{2} Z_i \rho Z_i \\ &= \frac{1}{2}\Big(|0\rangle^{\otimes n}\langle 0|^{\otimes n} + |1\rangle^{\otimes n}\langle 1|^{\otimes n} + (1-p_i)\Big(|0\rangle^{\otimes n}\langle 1|^{\otimes n} + |1\rangle^{\otimes n}\langle 0|^{\otimes n}\Big)\Big),\end{aligned}$$

it can be shown that the application of a noisy non local CNOT between server party and n parties takes their joint state to

$$\begin{aligned}\rho_{s,1,\ldots,n} \mapsto & \frac{1}{2}\Big(|0\rangle^{\otimes n+1}\langle 0|^{\otimes n+1} + |1\rangle^{\otimes n+1}\langle 1|^{\otimes n} \\ & + \prod_{i=0}^{n-1}(1-p_i)\Big(|0\rangle^{\otimes n+1}\langle 1|^{\otimes n+1} + |1\rangle^{\otimes n+1}\langle 0|^{\otimes n+1}\Big)\Big).\end{aligned}$$

Then, the parties input their corresponding data through the $\mathcal{Z}$ rotations of an angle θ_j. After that, a second distributed CNOT under dephasing noise with parameter takes the state of the server to state in 4, with $a = \prod_{i=0}^{n-1}(1-p_i)^2$

For *depolarising noise*, the same expression holds by replacing $\prod_{i=0}^{n-1}(1-p_i)$ by $1-(1-p_i)^2$. Note that for $n > 2$, applying an n-depolarizing channel gives a different result compared to applying a 1-depolarizing channel on all n qubits.

Let ρ_j be the state of the j-th server qubit. After entanglement generation and the first non local CNOT under depolarizing error with parameter $p_{i,1}$, the parties input their corresponding data by applying local $R_Z(\theta_j)$ gates. A second distributed CNOT under depolarizing noise with parameter $p_{i,2}$ gives

$$\begin{aligned}\rho_j &= (1-p_{i,1})\Big((1-p_{i,2})\rho'_j \otimes |0\rangle\langle 0|^n + \frac{p_{i,1}}{2}\mathrm{I}_{n+1}\Big) + \frac{p_{i,2}}{2}\mathrm{I}_{n+1} \\ &= \left((1-p_{i,1})(1-p_{i,2})\rho'_j \otimes |0\rangle\langle 0|^n + \frac{p_{i,1}(1-p_{i,2})+p_{i,1}}{2}\mathrm{I}_{n+1}\right)\end{aligned}$$

DOI: 10.1007/978-3-031-63778-0_26

with $\rho'_j = \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1| + e^{-i\theta_j} |0\rangle\langle 1| + e^{i\theta_j} |1\rangle\langle 0| \Big)$. Taking $p_{i,1} = p_{i,2} = p_i$, setting $a = 1-(1-p)^2$ and tracing out the degrees of freedom of the non server parties, we can write

$$\rho''_j = \mathbf{Tr}_{1\dots n}[\rho_j] = \frac{1}{2}\Big(|0\rangle\langle 0| + |1\rangle\langle 1| + ae^{-i\theta_j} |0\rangle\langle 1| + ae^{i\theta_j} |1\rangle\langle 0| \Big). \tag{10}$$

Theorem 1. *The m-player **DQA** protocol produces the output probability distribution such that for each potential output x*

$$P(x) = \frac{1}{2^n}\prod_{s=0}^{n-1}[1 + a\cos(\theta_s - 2\pi x/2^{n-s})], \tag{11}$$

with fidelity parameter $a \in [0,1]$ related to the depolarising or dephasing noise level in the shared GHZ states.

Proof. The state before the final inverse quantum Fourier transform is given by

$$|\Psi\rangle = \bigotimes_{s=0}^{n-1} \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_s}|1\rangle) = \bigotimes_{s=0}^{n-1}\frac{1}{\sqrt{2}}\left(\sum_{j_s=0,1} e^{i\theta_s j_s}|j_s\rangle\right), \tag{12}$$

which simplifies to

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} e^{i\sum_{s=0}^{n-1}\theta_s j_s}|j_{n-1}\dots j_0\rangle. \tag{13}$$

By Lemma 1, the presence of dephasing or depolarising noise on the quantum edges mixes the state of the server, such that the density matrix takes the form

$$\rho = \bigotimes_{s=0}^{n-1}\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + ae^{-i\theta_s}|0\rangle\langle 1| + ae^{i\theta_s}|1\rangle\langle 0|) \tag{14}$$

which can be written as

$$\rho = \frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{k=0}^{2^n-1} a^{\sum_s |k_s - j_s|} e^{i\sum_s(\theta_s j_s - \theta_s k_s)}|j_{n-1}\dots j_0\rangle\langle k_{n-1}\dots k_0|, \tag{15}$$

where $a = \tilde{a}^2$, as the distributed CNOT gates are performed twice, before and after the rotations.

The last step of the protocol consists of applying the inverse quantum Fourier transform. It maps the state in Equation (15) to

$$\begin{aligned}&\mathbf{IQFT}_n\rho\mathbf{QFT}_n\\ &= \frac{1}{2^{2n}}\sum_{x,y=0}^{2^n-1}\sum_{j,k=0}^{2^n-1} a^{\sum_s|k_s-j_s|}e^{i\sum_s\left(\theta_s - \frac{\pi}{2^s}x\right)j_s}e^{-i\sum_s\left(\theta_s-\frac{\pi}{2^s}y\right)k_s}|x_{n-1}\dots x_0\rangle\langle y_{n-1}\dots y_0|.\end{aligned} \tag{16}$$

ICCS Camera Ready Version 2024
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-63778-0_26

As the probability of measuring a computational basis state corresponds to the corresponding diagonal element of the density matrix, we obtain the probability $P(x)$ by setting $x = y$, completing the proof:

$$\begin{aligned} P(x) &= \frac{1}{2^{2n}} \prod_{s=0}^{n-1} \sum_{j_s,k_s=0,1} a^{|k_s-j_s|} e^{i\left(\theta_s - \frac{2\pi}{2^{n-s}}x\right)j_s} e^{-i\left(\theta_s - \frac{2\pi}{2^{n-s}}x\right)k_s} \\ &= \frac{1}{2^{2n}} \prod_{s=0}^{n-1} \left(1 + ae^{i\left(\theta_s - \frac{2\pi}{2^{n-s}}x\right)} + ae^{-i\left(\theta_s - \frac{2\pi}{2^{n-s}}x\right)} + 1\right) \\ &= \frac{1}{2^{n}} \prod_{s=0}^{n-1} \left[1 + a\cos\left(\theta_s - \frac{2\pi}{2^{n-s}}x\right)\right] . \end{aligned} \tag{17}$$

References

1. Aleksandrowicz, G., Alexander, T., Barkoutsos, P., Bello, L., Ben-Haim, Y., Bucher, D., et al.: Qiskit: An Open-source Framework for Quantum Computing (Feb 2019). https://doi.org/10.5281/zenodo.2562111
2. Arapinis, M., Lamprou, N., Kashefi, E., Pappa, A.: Definitions and security of quantum electronic voting. ACM Transactions on Quantum Computing **2**(1), 1–33 (2021)
3. Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J.A., Weinfurter, H.: Elementary gates for quantum computation. Phys. Rev. A **52**, 3457–3467 (11 1995). https://doi.org/10.1103/PhysRevA.52.3457
4. Beals, R., Brierley, S., Gray, O., Harrow, A.W., Kutin, S., Linden, N., Shepherd, D., Stather, M.: Efficient distributed quantum computing. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **469**(2153), 20120686 (May 2013). https://doi.org/10.1098/rspa.2012.0686
5. Caleffi, M., Amoretti, M., Ferrari, D., Cuomo, D., Illiano, J., Manzalini, A., Cacciapuoti, A.S.: Distributed quantum computing: a survey (2022)
6. van Dam, J.: Analytical Model of Satellite Based Entanglement Distribution. Master's thesis, TU Delft (2022)
7. DiAdamo, S., Ghibaudi, M., Cruise, J.: Distributed quantum computing and network control for accelerated vqe. IEEE Transactions on Quantum Engineering **2**, 1–21 (2021). https://doi.org/10.1109/TQE.2021.3057908
8. Draper, T.G.: Addition on a quantum computer (2000). https://doi.org/10.48550/ARXIV.QUANT-PH/0008033
9. Eisert, J., Jacobs, K., Papadopoulos, P., Plenio, M.B.: Optimal local implementation of nonlocal quantum gates. Phys. Rev. A **62**, 052317 (Oct 2000). https://doi.org/10.1103/PhysRevA.62.052317
10. Fedorov, A.K., Gelfand, M.S.: Towards practical applications in quantum computational biology. Nature Computational Science **1**(2), 114–119 (Feb 2021). https://doi.org/10.1038/s43588-021-00024-z
11. Gyongyosi, L., Imre, S.: Scalable distributed gate-model quantum computers. Scientific Reports **11**(1) (Feb 2021). https://doi.org/10.1038/s41598-020-76728-5

12. Harrow, A.W., Hassidim, A., Lloyd, S.: Quantum algorithm for linear systems of equations. Phys. Rev. Lett. **103**, 150502 (Oct 2009). https://doi.org/10.1103/PhysRevLett.103.150502
13. Hermans, S.L.N., Pompili, M., Beukers, H.K.C., Baier, S., Borregaard, J., Hanson, R.: Qubit teleportation between non-neighbouring nodes in a quantum network. Nature **605**(7911), 663–668 (may 2022). https://doi.org/10.1038/s41586-022-04697-y
14. Khabiboulline, E.T., Sandhu, J.S., Gambetta, M.U., Lukin, M.D., Borregaard, J.: Efficient quantum voting with information-theoretic security (2021). https://doi.org/10.48550/ARXIV.2112.14242
15. Li, Z., Liu, P., Zhao, P., Mi, Z., Xu, H., Liang, X., Su, T., Sun, W., Xue, G., Zhang, J.N., et al.: Error per single-qubit gate below 10^{-4} in a superconducting qubit. npj Quantum Information (2023). https://doi.org/10.1038/s41534-023-00781-x
16. Neumann, N.M.P., van Houte, R., Attema, T.: Imperfect distributed quantum phase estimation. In: Computational Science–ICCS 2020: 20th International Conference, Amsterdam, The Netherlands, June 3–5, 2020, Proceedings, Part VI 20. pp. 605–615. Springer (2020)
17. Neumann, N.M.P., Wezeman, R.S.: Distributed quantum machine learning. In: Innovations for Community Services. pp. 281–293. Springer International Publishing, Cham (2022)
18. Otero, A.R., Neumann, N.M.P., van der Schoot, W., Wezeman, R.: Noise robustness of a multiparty quantum summation protocol (2023). https://doi.org/10.48550/arXiv.2311.15314
19. Ruiz-Perez, L.; Garcia-Escartin, J.: Quantum arithmetic with the quantum fourier transform. Quantum Information Processing (2017). https://doi.org/10.1007/s11128-017-1603-1
20. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (nov 1979). https://doi.org/10.1145/359168.359176
21. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. **26**(5), 1484–1509 (1997). https://doi.org/10.1137/S0097539795293172
22. Wu, Q.L., Namekata, N., Inoue, S.: High-fidelity entanglement swapping at telecommunication wavelengths. Journal of Physics B: Atomic, Molecular and Optical Physics **46**(23), 235503 (nov 2013). https://doi.org/10.1088/0953-4075/46/23/235503
23. Xu, J.S., Yung, M.H., Xu, X.Y., Tang, J.S., Li, C.F., Guo, G.C.: Robust bidirectional links for photonic quantum networks. Science Advances **2**(1), e1500672 (2016). https://doi.org/10.1126/sciadv.1500672
24. Yimsiriwattana, A., Jr., S.J.L.: Distributed quantum computing: a distributed Shor algorithm. In: Donkor, E., Pirich, A.R., Brandt, H.E. (eds.) Quantum Information and Computation II. vol. 5436, pp. 360 – 372. International Society for Optics and Photonics, SPIE (2004). https://doi.org/10.1117/12.546504
25. Yimsiriwattana, A., Lomonaco, S.J.: Generalized GHZ states and distributed quantum computing (2004). https://doi.org/10.48550/ARXIV.QUANT-PH/0402148
26. Šafránek, D., Ahmadi, M., Fuentes, I.: Quantum parameter estimation with imperfect reference frames. New Journal of Physics **17**(3), 033012 (mar 2015). https://doi.org/10.1088/1367-2630/17/3/033012