Blind Calibration of Quantum Devices over Noisy Quantum Channels

Ankit Khandelwal, Stephen DiAdamo

Abstract—To mitigate the noise in quantum channels, calibration is used to tune the communication system to minimize error. Generally, calibration is performed by transmitting pre-agreed-upon calibration states and determining an error cost so the two parties can tune their devices accordingly. The calibration states can be the same ones used for the desired protocol and so an untrusted party could potentially learn which protocol is being performed by gathering knowledge of the calibration states and cost function. Here, we assume an insecure quantum channel and therefore the receiver should not be allowed to determine the calibration states, but is honest in announcing the measurement results to the sender. We limit the classical information that is openly transmitted and in this regard, we propose a simple protocol that hides the calibration states and cost function from the receiver, but still allows for calibration to be performed efficiently. We show various numerical results demonstrating the ability of the protocol under various channel noise parameters and communication scenarios.

Index Terms—Calibration, quantum communication, secure communication.

I. INTRODUCTION

Quantum network technologies are rapidly developing in various directions and the potential applications for quantum networks are becoming more realistic for commercial deployment. A key benefit quantum networks bring is an unreachable level of security that classical networks cannot currently achieve, with protocols such as quantum key distribution [1], secret sharing [2], and blind quantum computing [3]. A similarity that each of these protocols share is that, before the protocols begins, and periodically during a continuous execution, the communicating parties perform a device calibration protocol to ensure their transmission and detection devices are aligned, minimizing any noise-induced errors caused by the quantum channel. Optical components are affected by environmental changes like temperature fluctuations [4], and so it is necessary to regularly calibrate the devices to mitigate these effects.

By performing calibration, it opens the network up to potential attack. For example, in the security proofs of some QKD protocols, it is assumed that the devices begin in a calibrated state, but it has been shown that there are attacks that can be performed during the calibration protocol [5], [6], thereby diminishing the security. Further, in QKD it is critical that an accurate estimate for the Quantum Bit Error Rate (QBER) is known so that information reconciliation can be accurately and efficiently performed [7], and so calibration is essential. It is therefore important for the calibration stage to be as secure as the protocols themselves.

An approach to device calibration for quantum communication is to align the transmitter and receiver using polarized states as described in [8], where the sender and receiver tune a polarization controller to calibrate the channel, where the sender and receiver both know the calibration states. Here we propose a calibration strategy that uses the same quantum signals that will be used in the protocol to be executed, allowing calibration, but done in a way such that the receiver cannot determine the states, thereby protecting the secrecy of the protocol.

In this work, we propose a simple approach to overcoming the need for the sender to reveal the calibration states and the cost function used for calibration. We call this approach “blind calibration” because from the perspective of the receiver, they are blind to which quantum states they are receiving and why the tuning of their device is improving transmission cost. The approach here is to randomize the transmission order of the calibration states using different probability distributions, thereby preventing the receiver from performing quantum state tomography. Moreover, the sender hides the cost function by computing it at the their side of the channel, sending only a—potentially obfuscated—value back to the receiver. The sender’s goal is to perform the calibration as efficiently as possible, hiding as much information as possible. In this work, we propose a communication protocol that achieves this goal and we analyze various transmission scenarios for proof-of-concept. With simulation, we test how well our approach works over fiber channel models with various noise parameters.

Throughout this work we use the following mathematical notation. The set of quantum states on a finite dimensional, complex Hilbert space \( \mathcal{H} \) is denoted \( S(\mathcal{H}) \). The set of probability distributions on a set \( S \) is denoted \( \mathcal{P}(S) \). A quantum channel is a Completely Positive Trace Preserving (CPTP) map over the state space \( S(\mathcal{H}) \). Random variables are usually denoted as \( X_i \) and vectors of random variables with a bold-face notation \( \mathbf{X} \).

II. BLIND CALIBRATION OVER QUANTUM CHANNELS

In this section, we introduce our protocol for blind calibration. In order to specify the protocol, we need to firstly state the assumptions we make. Similar to the main assumptions for many quantum cryptographic protocols, we assume the following: 1) Quantum theory is correct, particularly that the no-cloning theorem holds; 2) Both parties act to achieve the goal of the protocol and do not act to prevent it from being fulfilled; 3) The sender has a trusted and private random number generator; 4) The sender operates in a secure location and particularly their quantum source has no side channels leaking information.

With these assumptions, we state our protocol for blind calibration. In Protocol 1, we list the the protocol instructions...
for the sender and receiver. The high level idea of the protocol is that the sender obfuscates the transmission statistics in order to prevent the receiver from performing tomography [9], but at the same time, using efficient optimization algorithms to find the tuning parameters that minimize the desired cost function. To do this, for each iteration of the protocol, the sender selects a new distribution $p \in P(S)$ to determine the order to transmit $N$ quantum states, where $S$ forms a set of calibration states. From there, $N$ transmissions are made to the receiver after being processed by an encoder, and the receiver then performs a decoding operation and measures in a particular basis. The measurement results are sent back to the sender with the basis information, and a cost of transmission is determined by the sender. The cost is used to update the encoding strategy and is further sent to the receiver to update the decoding strategy. This process repeats until convergence or a maximum number of iterations $I_{\text{max}}$ is reached. In this sense, any eavesdropper intercepting the quantum states in transmission cannot perform a tomography attack to determine which quantum states are being transmitted.

We further justify why tomography at the receiver alone cannot be performed on the transmitted states to uncover the calibration state set $S$. The original algorithm for tomography is as follows. For a density matrix $\rho$ from a Hilbert space of $n$ dimensions, we have the following equation,

$$\rho = \frac{1}{2^n} \sum_{v} \text{Tr}(\sigma_{v_1} \otimes \cdots \otimes \sigma_{v_n}) \sigma_{v_1} \otimes \cdots \otimes \sigma_{v_n}.$$  

(1)

Here, the vectors $\vec{v} = (v_1, \ldots, v_n)$ with entries $v_i$ are taken from the set $\{I, X, Y, Z\}$ of Pauli matrices. For a single qubit, the basis set has 4 components, for $n$ qubits, the basis set has $4^n$ components. Thus, the number of measurements that the receiver has to perform increases exponentially with $n$. Now, in order to reconstruct a density matrix with tomography, it is assumed that the state on which tomography is being performed is the same for each measurement. In our protocol, we ensure that the receiver is unable to determine when, from a set of calibration states, a specific quantum state was transmitted because each state is transmitted according to a random distribution. The best the receiver can do is compute an average state matrix, but the average state cannot reveal state information of the parts. Moreover, between iterations, the random variable determining the probability of a calibration state being transmitted changes, and so the average density matrix will vary iteration to iteration, further obfuscating the calibration states. With larger quantum systems, tomography requires even more measurement basis, further complicating the task of state reconstruction.

III. System Model and Simulation Configuration

In this section, we present a model for a communication system that performs Protocol 1. The components of the system are a quantum source, an encoding device, the noisy quantum channel, a decoding device, and a measurement device. To model these components, we use the following. For simplicity of analysis, we assume that the quantum source emits quantum states with perfect fidelity, and therefore there is no noise model associated with it. For the encoder and decoder, we assume that they are quantum channels parameterized by a vector of variables $\theta^i = (\theta^i_0, \theta^i_1, ..., \theta^i_n)$ for the encoder and $\phi^i = (\phi^i_0, \phi^i_1, ..., \phi^i_m)$ for the decoder, where the superscript $i$ represents the current iteration of the protocol. For the measurement device, we again assume for simplicity that measurement outcomes are accurate.

For the quantum channel, we consider noise models for coherent noise. Firstly we model random noise by applying small, random, unitaly rotations, and secondly we consider length-dependent bit- and phase-flip errors. The noise models are applied via quantum channels such that each qubit in the system has an independent chance of experiencing the noise.

For the rotational noise model, we generate a random rotation vector $\theta^i_0$ with elements from $-\pi$ to $\pi$. Then, depending on the length $L$ kilometers of the channel, we determine the percentage of the rotation applied via, $p = 1 - 10^{-\mu L}$, where $\mu$ is a parameter of the channel. For the length-dependent noise,
for a channel of length $L$ and channel parameters $\mu_1, \mu_2 \geq 0$, the probability that a qubit arrives with a bit-flip error or a phase-flip error is $p_b = 1 - 10^{-\mu_1 L}$ and $p_p = 1 - 10^{-\mu_2 L}$ respectively.

For the protocol, we need to select a cost function. Here any valid cost function can work, but in our simulations, we use the quantum fidelity and error rates. Fidelity between states is defined as follows. Assuming the input state is $\sigma \in S(\mathcal{H})$ and the output state is $\rho \in S(\mathcal{H})$, the state fidelity between the two is given by,

$$F(\rho, \sigma) := \text{Tr} \left( \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right)^2.$$

To use fidelity a cost, we define infidelity to be $1 - F$. In order to determine the fidelity in simulation, we implemented quantum state tomography [9] as explained in the previous section. In order compute the fidelity nonlocally in our case, the receiver needs to perform the measurements and the sender needs to perform the state reconstruction to compute the state fidelities of the calibration states. This process is much the same as the original algorithm, it differs only in that the measurement outcomes are sent back to the sender for state reconstruction instead being determined computed locally.

The error rates as a cost function are calculated by comparing the classical input to the measured output. For an input vector $\text{in}$ of classical messages and output $\text{out}$, the error rate is computed as,

$$\text{err}(\text{in}, \text{out}) := 1 - \frac{1}{n} \sum_{i=1}^{n} \delta_i(\text{in}, \text{out}),$$

where $\delta_i(a, b) = 1$ if $a_i = b_i$ and 0 otherwise and $n = |\text{in}| = |\text{out}|$.

To numerically analyze Protocol 1, we use a collection of simulated experiments developed using the quantum computing framework PennyLane [10]. PennyLane is a simulation framework for performing differential programming of quantum computers, and can be efficiently used for optimization tasks in quantum computing. We configure our simulations as follows. We begin by generating a parameterized quantum circuit in PennyLane that performs the encoding step, the quantum channel, the decoding step, and the measurements. For updating the encoder and decoder parameters, after each iteration, updated values are passed to the circuit. For the update function, we use an optimizer to minimize the cost function. Here, any optimizer can work, but for our simulations, we use the Adam optimizer [11]. The encoder and decoder parameters are then updated during protocol execution according to the optimizer outputs. For noise parameters, depending on the length of the channel, we provide the circuit a set of parameters for the rotational and probabilistic bit- or phase-flip noise values. The parameters of the protocol and the set of calibration states are chosen and then simulation can run.

IV. PROTOCOL PERFORMANCE BENCHMARKS

We benchmark the performance of Protocol 1 for various communication scenarios under typical noise parameters for fiber communication. To simplify the simulation model, we assume that the sender simply prepares quantum sources but does not modify their encoding during the protocol. In our notation, this implies $E_{\mu_i}$ is the identity for all iterations $i$. Indeed, with tuning ability, a sender can pre-calibrate their device locally, ensuring the states they intend to transmit are calibrated to their standard, and so generality is not lost with this assumption.

A. Random Single-Qubit States

As an initial test of the protocol, we analyze the case where the sender randomly selects $n = 5$ single-qubit states for transmission. During transmission, the receiver measures the incoming states in one of the three Pauli bases such that quantum state tomography can be performed at the sender’s side. For a cost function, the sender computes an average state fidelity using the measurements from the receiver to compare against the originally chosen states.

For this test of the protocol, we fix the length of the fiber to 50 km and determine how many iterations of the protocol are needed for approximate convergence to determine a good parameter regime for a more in-depth study of the protocol that we conduct in the later sections. The number of states transmitted per iteration here is $N = 15,000$. For this analysis, we use a simple rotational noise model which rotates qubits as defined above with $\mu = 0.005$. We then deterministically apply a Bloch sphere rotation $p \cdot \theta R_k$ to each qubit that travels through the channel. For decoding, we apply a counter rotational correction before a measurement is made. In Fig. 1, we can see that with approximately 100 iterations of the protocol, the protocol has learned how to overcome the rotational noise effects in the channel. Based on these results, for the remainder of this work, we use $I_{\text{max}} = 250$ iterations for our simulations unless otherwise stated.

B. BB84 States

The BB84 protocol uses states $\{0, 1, +, -\}$ and transmits them with equal probability. A naive calibration process is to tell the receiver the basis in which the state is prepared and repeatedly transmit the state. The receiver can then tune the decoder according to a quantum bit error rate and this can be repeated for all states. The receiver then knows exactly which states are the protocol states and what the cost function is, and with this information, the receiver (or an eavesdropper imitating the receiver), can predict the protocol the sender intends to perform. Using Protocol 1 instead, the sender need not disclose the calibration states nor the cost.
function, thereby masking the protocol parameters from the receiver, preventing the receiver from learning which protocol the sender intends to perform.

The QKD results after performing Protocol 1 for a channel with only rotational noise are plotted in Fig. 2 (a). We can see that as the fiber distance increases, the QBER will tend to 0.6 in the pre-calibrated stage (blue). Using Protocol 1 to calibrate the system, the trained decoder reduces the BB84 QBER in the system nearly entirely within 250 iterations of training with 1,000 (lossless) transmissions per iteration. In Fig. 2 (b) is the performance over a channel that has both rotational noise and probabilistic bit- and phase-flip error. What we can see is that until roughly 60 km, calibration makes no difference to accommodate the noise in the channel, since the probability of the error applying is smaller than 0.5. Once the flipping probability exceeds 0.5, the QBER can be minimized by applying the inverse rotations deterministically.

We further test how many transmissions are required in order to minimize the QBER within 20 iterations, as the number of transmissions build up accuracy in the statistics regarding the noise properties of the channel. The results appear in Fig. 3. We assume that the both the sender and receiver transmit half of a Bell pair to a central node, and the sender selects a Bell state at random. The central node performs a correction to overcome channel noise before measuring, but is unaware of which Bell state is being distributed. The central node performs a Bell state measurement on the incoming qubits. To teleport the quantum state, two classical bits used for correction are sent to one party. After this, the sender and receiver parties measure their remaining half and can coordinate with each other to generate a cost function, which in this case is as defined in Eq. (3), where the input is Bell states that were transmitted, and the output is the resultant measured Bell pair.

We perform Protocol 1 over two error models. In Fig. 4 (a), we analyze the effect of arbitrary rotation. In the Fig. 4 (b), we include bit- and phase-flip error. With deterministic errors, as are the arbitrary rotations, it is possible to correct for error. For probabilistic error, we see that until the probability is high enough for error, no correction using rotational correction can be effectively applied. Once it is the case, we see the calibrated error rates diverge from the uncorrected error rates. Here again we do not simulate loss, and a scaling factor should be applied to accommodate loss as explained in Section IV-B for each channel and for detector flaws.

D. Multiparticle Entanglement Distribution

We simulate a communication setting for transmitting multiparticle entanglement, specifically GHZ and W states, over channels with rotational noise. GHZ states and W states are defined as, $|GHZ⟩ := \frac{1}{\sqrt{2}}(|000⟩ + |111⟩)$ and $|W⟩ := \frac{1}{\sqrt{N}}(|000⟩ + |010⟩ + |100⟩ + |001⟩)$. GHZ states and W states are important for protocols like quantum secret sharing [2], anonymous transmission [14], [15], and others.
Here we analyze a setting where a sender prepares $n$ qubit GHZ or W states and transmits them over a noisy channel.

In Fig. 5, we show the calibration effects for correcting the channel noise for both a varying number of qubits in the entangled quantum systems and length of the channel. With a growing number of qubits in the system, there is a higher rate of infidelity, but as with the previous results, we see that the protocol can robustly correct deterministic errors in the channel. Here we have used the state infidelity as the cost, approximating the output state density matrix using multi-qubit state tomography in Eq. (1). For better performance of the simulation, we use $\varepsilon_{\text{inf}} = 10^{-5}$ and 20,000 channel transmissions per protocol iteration. Here we do not simulate probabilistic noise, as simulation performance rapidly deteriorates with larger entangled states, but given the noise models are the same as the previous cases, we suspect a similar trend would emerge, where until roughly $L = 60$ km no corrections can be made.

**V. Conclusion**

In conclusion, we have shown that it is possible to mask the calibration states and cost, while still allowing the calibration to take place. To accomplish this, we proposed the Blind Calibration protocol which randomizes the transmission order, preventing any other party from performing state tomography in order to learn the calibration state set. By performing the calibration cost at the sender’s side, there is further masking of the calibration protocol, minimizing any leakage of the calibration protocol to any malicious parties. We show that, under various communication settings, the protocol works well even under noisy channel conditions. In our analysis, we used simple decoding strategies to overcome noise, but more complex strategies can directly fit with the protocol framework. The protocol we propose is general and accommodates any quantum communication setting where calibration is required making it practical and timely during the growing interest in quantum communication and quantum networks.

**REFERENCES**

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Luo, C. Ottaviani et al., “Advances in quantum cryptography,” *Advances in optics and photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[2] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[3] J. F. Fitzsimons, “Private quantum computation: an introduction to blind quantum computing and related protocols,” npj Quantum Information, vol. 3, no. 1, pp. 1–11, 2017.

[4] W. F. Yeung and A. R. Johnston, “Effect of temperature on optical fiber transmission,” *Applied optics*, vol. 17, no. 23, pp. 3703–3705, 1978.

[5] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, “Device calibration impacts security of quantum key distribution,” *Physical Review Letters*, vol. 107, no. 11, p. 110501, 2011.

[6] Y.-Y. Fei, X.-D. Meng, M. Gao, H. Wang, and Z. Ma, “Quantum man-in-the-middle attack on the calibration process of quantum key distribution,” *Scientific reports*, vol. 8, no. 1, pp. 1–10, 2018.

[7] D. Elkouss, J. Martínez-Mateo, and V. Martin, “Information reconciliation for quantum key distribution,” *arXiv preprint arXiv:1007.1616*, 2010.

[8] G. Xavier, N. Walenta, G. V. de Faria, G. Temporão, N. Gisin, H. Zbinden, and J.-P. Von Der Weid, “Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation,” *New Journal of Physics*, vol. 11, no. 4, p. 045015, 2009.

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

[10] V. Bergholm, J. Izaac, M. Schuld, C. Gogolin, M. S. Alam, S. Ahmed, J. M. Arrazola, C. Blank, A. Delgado, S. Jahangiri et al., “Pennylane: Automatic differentiation of hybrid quantum-classical computations,” *arXiv preprint arXiv:1811.04968*, 2018.

[11] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” *arXiv preprint arXiv:1412.6980*, 2014.

[12] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, “‘3-event-ready-detectors’ bell experiment via entanglement swapping,” *Physical Review Letters*, vol. 71, no. 26, 1993.

[13] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Physical review letters*, vol. 108, no. 13, p. 130503, 2012.

[14] V. Lipińska, G. Murta, and S. Wehner, “Anonymous transmission in a noisy quantum network using the w state,” *Physical Review A*, vol. 98, no. 5, p. 052320, 2018.
[15] M. Christandl and S. Wehner. “Quantum anonymous transmissions,” in *International conference on the theory and application of cryptology and information security*. Springer, 2005, pp. 217–235.