Estimating Sources for Weak-Coherent-State-Based Quantum Key Distribution

J. L. E. Silva and H. M. Vasconcelos

***Abstract*— Quantum key distribution allows two parties to generate a shared cryptographic key of bits such that an eavesdropper is not able to obtain significant information about the key without being detected. In protocols based on the transmission of coherent states, the error rate, the key rate generation, and the system security depend on the source states used. In here, we show that quantum homodyne tomography using discretization of the measurements into histogram bin can be used as an estimator to analyze the aforementioned source states without losing too much information.**

***Keywords*— Quantum key distribution, Coherent states, Estimator.**

I. Introduction

Quantum information technology has advanced to the point where Quantum Key Distribution (QKD) and rudimentary quantum computers are commercially available [1], [2], [3], [4]. Quantum computation and quantum internet using telecommunications band, in particular, have achieve a milestone with the demonstration of a telecom-band CNOT gate [7] and the improvement of the storage time of a telecom-compatible quantum memory [8].

QKD is a modern form of trusted communication, which in principle allows a secure transmission of a message between a sender (Alice) and a receiver (Bob). The two parties establish a secure key by transmitting quantum states through an insecure channel. Any attack realized by an eavesdropper (Eve) disturbs the transmitted quantum state and can be detected [5], [6]. QKD schemes using single photons or pairs of entangled photons are highly secure [9]. However, single photons or pairs of photons can be easily absorbed, limiting the key rate generation and operational distance of these schemes. The use of higher intensity signals is an obvious alternative to circumvent these limitations, and most importantly, it also ensures that any eavesdropping will be detectable [10], [11], [12].

The safety of a quantum key distribution protocol depends on the fact that any attempt to eavesdrop on the quantum channel generates errors in the transmission. For a given error rate, the system itself and the eavesdropping strategy determine the amount of information that may have leaked to the eavesdropper. In protocols based on the transmission of coherent states, the error rate, the key rate generation, and the system security depend on the source states used. In general, it is necessary to generate the source states $\alpha\, e^{i\phi}$, where α is assumed to be real and the phases take one of four possible values, $0, \pi/2, \pi, 3\pi/2$. Consequently, precise reconstruction and diagnostic tools to estimate quantum states [13], [14], [15], [16], [17] are fundamental.

In the quantum homodyne tomography considered here, measurements are performed on each member of a collection of source states prepared in the same state. The idea is to estimate the source states from the experimental measurements results. The estimation can be done using a range of different methods. We used Maximum Likelihood Estimation (MLE), that finds among all possible candidate states, the one which maximizes the probability of obtaining the experimental data set. For the likelihood maximization, we propose the use of an algorithm with interactions of the $R\rho R$ algorithm followed by iterations of a regularized gradient ascent algorithm (RGA).

A homodyne measurement generates a continuous value. In general, discretization of data is not necessary, but it can save time in the reconstruction algorithm due to the reduction of the number of data. We showed here that quantum homodyne tomography using discretization of the measurements into histogram bin can be used as a powerful tool to estimate coherent states sources for QKD.

II. Description of the Estimator

To estimate a coherent state source of a QKD scheme we need N quantum systems, each of them prepared in the coherent state described by a density matrix ρ_{true}. We perform N experimental trials and in each trial i we measure the field quadrature of one of the systems at some phase θ_i of a local oscillator. If we measure a quadrature value x_i, for a given phase θ_i, the resulting data will be $\{(\theta_i, x_i)|i = 1, \ldots, N\}$.

For a certain candidate density matrix ρ, the probability of obtaining outcome x_i, when measuring with phase θ_i, is given by Born's rule: $\mathrm{Tr}(\rho\Pi_i)$, where $\Pi_i = \Pi(x_i|\theta_i)$ is the positive-operator-valued measure (POVM) element associated with the outcome of the i-th measurement. Given the data, the likelihood of a candidate density matrix ρ is

$$\mathcal{L}(\rho) = \prod_{i=1}^{N} \mathrm{Tr}(\Pi_i \rho). \tag{1}$$

MLE searches for the density matrix that maximizes the likelihood in Eq. (1). The same density matrix that maximizes the likelihood also maximizes the "log-likelihood", given by

$$L(\rho) = \ln \mathcal{L}(\rho) = \sum_{i=1}^{N} \ln[\mathrm{Tr}(\Pi_i \rho)]. \tag{2}$$

Since this function is concave and convergence to a unique solution will be achieved by most iterative optimization methods, we usually choose to maximize the log-likelihood.

J. L. E. Silva and H. M. Vasconcelos Universidade Federal do Ceará, Fortaleza, Brazil, E-mail: hilma@ufc.br.

We propose the use of an algorithm for likelihood maximization that begins with interactions of the $R\rho R$ algorithm [19] followed by iterations of a regularized gradient ascent algorithm (RGA). The change is due to an expressive slow-down of the $R\rho R$ algorithm after about $(n+1)^2/4$ iterations. In the RGA, $\rho^{(k+1)}$ is parametrized as

$$\rho^{(k+1)} = \frac{\left(\sqrt{\rho^{(k)}} + A\right)\left(\sqrt{\rho^{(k)}} + A^\dagger\right)}{\mathrm{Tr}\left[\left(\sqrt{\rho^{(k)}} + A\right)\left(\sqrt{\rho^{(k)}} + A^\dagger\right)\right]}, \qquad (3)$$

where $\rho^{(k)}$ is the density found by the last interaction of $R\rho R$, and A may be any complex matrix of the same dimensions as ρ. The density matrix $\rho^{(k+1)}$ is a physical density matrix for any chosen A. The matrix A maximizes the quadratic approximation of the log-likelihood subject to $\mathrm{Tr}(AA^\dagger) \leq u$, where u is a positive number adjusted by the algorithm, such that the log-likelihood increases with each iteration. The stopping criterion $L(\rho_{\mathrm{ML}}) - L(\rho^{(k)}) \leq 0.2$, where $L(\rho_{\mathrm{ML}})$ is the maximum of the log-likelihood, is used to halt the interactions [18].

III. Results

Our numerical experiments simulate single mode optical homodyne measurements of coherent states. Each considered state is represented by a density matrix ρ_{true} in an n photon basis. To better simulate realistic experiments, these pure coherent states are subject to a 0.05 photon loss before measurement. We also include photon detector inefficiency by considering detectors with efficiency $\eta \sim 0.9$. To guarantee random samples of homodyne measurement results, we use rejection sampling from the distribution given by $P(x|\theta)$ [20].

The homodyne measurements are performed at m phases, where m divides the upper-half-circle (between 0 and π) evenly. We measure N/m times at each phase, where N is the total number of measurements. We use $N = 20,000$ e $m = 20$ in our simulations. In each case studied here, we simulate 100 tomography experiments, making 100 density matrix estimates. The graphs show the arithmetic mean of the 100 fidelities of the reconstructed states. The error bars show the standard deviation of the 100 fidelities.

Fig. 1 shows the average fidelity as a function of the bin width used to discretize the data when reconstructing a coherent state with $\alpha = 1$ and $\phi = 0$ in the expression of the source states, $\alpha\, e^{i\phi}$. Fig. 2 shows the average fidelity as a function of the bin width for a coherent state with $\alpha = 0.1$ and $\phi = \pi/2$. In both cases, the state is reconstructed in a Hilbert space truncated at $n = 10$ photons, and every measurement outcome in a given bin has been associated with the measurement operator for the quadrature value at the center of that bin.

As expected, the highest fidelities occur when we do not discretize the available data. We also see in Figs. 1 and 2 that smaller bin widths result in higher fidelities. However, when compared to the raw data, the smallest bin widths tested result in a fidelity loss of only 0.002. The loss in fidelity when using the largest bin widths was of about 0.23. As we can see, the choice of bin width is essential in guaranteeing a smaller loss of information. Ideally, when we use discretization of the measurement results, we should seek a method to determine an optimal bin width. On the other hand, when using discretization, we get much faster fidelity estimates. For example, the slowest reconstruction when using discretization is 20 times faster than reconstructing using all the data.

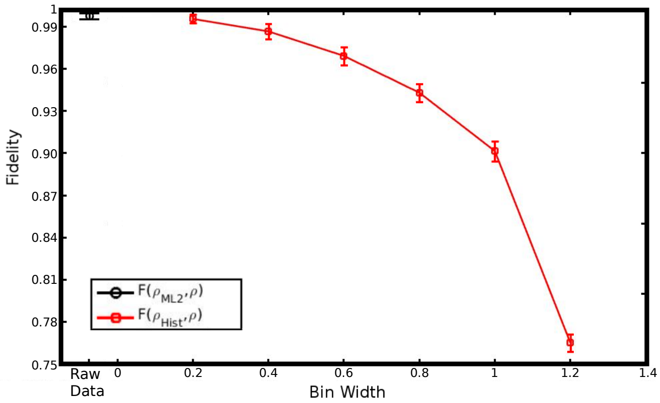

Fig. 1. Average fidelity as a function of the bin width for a coherent state with $\alpha = 1$ and $\phi = 0$. The Hilbert space is truncated at $n = 10$ photons.

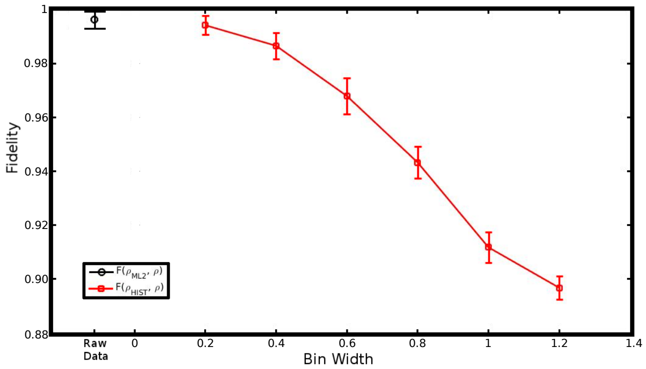

Fig. 2. Average fidelity as a function of the bin width for a coherent state with $\alpha = 0.1$ and $\phi = \pi/2$. The Hilbert space is truncated at $n = 10$ photons.

IV. Conclusions

We have shown that quantum homodyne tomography using histograms can be used as efficient estimator to analyze coherent-state-based QKD source states without loosing too much information. We plan, in a future work, to study different strategies to choose optimal quadrature bin widths and to analyze the impact of integrating the measurement operators along the length of the bin.

Acknowledgments

We thank Prof. Rubens Ramos for helpful comments on the manuscript. H. M. Vasconcelos thanks the Schlumberger Foundation's Faculty for the Future program for financial support. J. L. E. Silva thanks Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) for financial support.

References

[1] L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 156 (2012).

[2] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, "Hardware-efficient Quantum Optimizer for Small Molecules and Quantum Magnets," *Nature*, **549**, 242-246 (2014).

[3] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Experimental comparison of two quantum computing architectures," *Proc. Natl. Acad. Sci. U. S. A.*, **114**, 3305-3310 (2017).

[4] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable shor algorithm," *Science*, **351**, 1068-1070 (2017).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, **81**, 1301 (2009).

[6] Hoi-Kwong Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photonics*, **8**, 595 (2014).

[7] J. Chen, J. B. Altepeter, M. Medic, K. F. Lee, B. Gokden, R. H. Hadfield, S. W. Nam, and P. Kumar, "Demonstration of a Quantum Controlled-NOT Gate in the Telecommunications Band," *Phys. Rev. Lett.*, **100**, 133603 (2008).

[8] M. Rančić, M. P. Hedges, R. L. Ahlefeldt, and M. J. Sellars, "Coherence time of over a second in a telecom-compatible quantum memory storage material," *Nature Phys.*, **14**, 50-54 (2018).

[9] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, **85**, 441 (2000).

[10] P. V. P. Pinheiro, R. V. Ramos, "Quantum communication with photon-added coherent states," *Quantum Inf. Processing*, **12**, 537-547 (2013).

[11] D. S. Simon, G. Jaeger, and A. V. Sergienko, "Entangled-coherent-state quantum key distribution with entanglement witnessing," *Phys. Rev. A*, **89**, 012315 (2014).

[12] G. Jaeger, D. S. Simon, A. V. Sergienko, "Coherent state quantum key distribution based on entanglement sudden death," *Quantum Inf. Processing*, **15**, 1117-1133 (2016).

[13] K. Vogel and H. Risken, "Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase," *Phys. Rev. A*, **40**, 2847-2849 (1989).

[14] T. Dunn, I. A. Walmsley, and S. Mukamel, "Experimental determination of the quantum-mechanical state of a molecular vibrational mode using fluorescence tomography," *Phys. Rev. Lett.*, **74**, 884-887 (1995).

[15] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi, "Maximum-likelihood estimation of the density matrix," *Phys. Rev. A*, **61**, 010304(R) (2000).

[16] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, "Exploring Hilbert space: Accurate characterization of quantum information," *Phys. Rev. A*, **65**, 012301 (2002).

[17] A. Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier, "Generation of optical 'Schrödinger cats' from photon number states," *Nature*, **448**, 784-786 (2007).

[18] S. C. Glancy, E. Knill, and M. Girard, "Gradient-based stopping rules for maximum-likelihood quantum-state tomography," *New J. Phys.*, **14**, 095017 (2012).

[19] J. Řeháček, Z. Hradil, E. Knill and A. I. Lvovsky, "Diluted maximum-likelihood algorithm for quantum tomography," *Phys. Rev. A*, **75**, 042108 (2007).

[20] W. J. Kennedy Jr. and J. E. Gentle, *Statistical Computing*, Marcel Dekker, Inc. (1980).

[21] G. B. Silva, S. Glancy, and H. M. Vasconcelos, "Investigating bias in maximum-likelihood quantum-state tomography," *Phys. Rev. A*, **95**, 022107 (2007).