Efficient quantum communications with coherent state fingerprints

Niraj Kumar,[1,2] Adeline Orieux,[1,2] Eleni Diamanti,[1] and Iordanis Kerenidis[2,3]

[1]*LIP6, CNRS, Université Pierre et Marie Curie, Sorbonne Universités, 75005 Paris, France*
[2]*IRIF, CNRS, Université Paris Diderot, Sorbonne Paris Cité, 75013 Paris, France*
[3]*CQT, National University of Singapore, Singapore*

Communication complexity is an ideal model for testing quantum mechanics and for understanding the efficiency of quantum networks. This model studies the amount of communication required by separate parties to jointly compute a task. There are several examples where communicating quantum information can result in considerable savings in the communication overhead [1, 2]. Nevertheless, it is in general difficult to test these results experimentally and demonstrate quantum superiority in practice since the quantum protocols typically necessitate large, highly entangled states, which are out of reach of current photonic technologies.

Recently, Arrazola and Lütkenhaus proposed a mapping for encoding quantum communication protocols involving pure states of many qubits, unitary operations and projective measurements to protocols based on coherent states of light in a superposition of optical modes, linear optics operations and single-photon detection. This powerful model was used to propose the practical implementation of coherent state quantum fingerprints, leading to two experimental demonstrations: a proof-of-principle use of such fingerprints for solving the communication task of Equality asymptotically better than the best known classical protocol with respect to the transmitted information [3]; and a subsequent implementation beating the classical lower bound for the transmitted information [4]. Following these demonstrations that have focused on Equality and on transmitted information, an important question remains: is there a realistic model for proving and testing in practice that quantum information is asymptotically better than classical for communication tasks with respect to *all* important communication and information resources?

We answer in the affirmative by proposing the *first example of a communication model and a distributed task, for which there exists a realistic quantum protocol that is asymptotically more efficient than any classical protocol, both in the communication and the information resources.* For this, we extend a recently proposed coherent state mapping for quantum communication protocols, study the use of coherent state fingerprints over multiple channels and show their role in the design of an efficient quantum protocol for estimating the Euclidean distance of two real vectors within a constant factor.

Our communication model is as follows. Alice and Bob possess large data sets x and y respectively, which are unit vectors in $\mathcal{R}^n$. They would like to allow a Referee to check how similar their data is by estimating the Euclidean distance. We call this the Euclidean Distance problem. Alice and Bob can transmit their entire data to the Referee, but this is non-optimal. The idea is to send fingerprints of the data, which are much shorter but still allow the Referee to approximate their Euclidean distance within some additive constant. Such a model also requires the Referee to receive the fingerprints of data of both players at the same time.

We come up with a new scheme for experimental implementation of the quantum fingerprinting protocol for estimating the Euclidean distance. This implementation is in sharp contrast with the previous proof-of-principle fingerprinting experiments in a way that we have completely separate paths for Alice and Bob, as opposed to previous implementations which involved the sagnac loop setup where Alice's pulse passes through Bob's path and vice-verca. Although the sagnac loop makes sure that the players pulses arrive to the Referee at the same time, but it might compromise on the fact that a possibility of communication between the two players during the protocol run might arise. We overcome this issue by carefully adjusting the path lengths of Alice and Bob to makes sure the pulses arrive to the Referee at the same time. We give preliminary results based on this setup for Equality and Euclidean distance protocols.

Further details on our model and the scheme can be found on[5].

[1] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[2] D. Gavinsky, arXiv preprint arXiv:1602.05059 (2016).
[3] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus, and H.-K. Lo, Nature Commun. **6**, 8735 (2015).
[4] J.-Y. Guan, F. Xu, H.-L. Yin, Y. Li, W.-J. Zhang, S.-J. Chen, X.-Y. Yang, L. Li, L.-X. You, T.-Y. Chen, et al., Phys. Rev. Lett. **116**, 240502 (2016).
[5] N. Kumar, E. Diamanti, and I. Kerenidis, Physical Review A **95**, 032337 (2017).