Experimental Quantum Fingerprinting

Feihu Xu,[1,*] Juan Miguel Arrazola,[2,*] Kejin Wei,[1,3] Wenyuan Wang,[1,4] Pablo Palacios-Avila,[2,5] Chen Feng,[6] Shihan Sajeed,[2] Norbert Lütkenhaus,[2] and Hoi-Kwong Lo[1]

[1]*Center for Quantum Information and Quantum Control (CQIQC), Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*[†]
[2]*Institute for Quantum Computing (IQC), University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada*
[3]*School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876*
[4]*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong, China*
[5]*Facultad de Ciencias, Universidad Nacional de Ingenieria, Lima, Peru.*
[6]*School of Engineering, University of British Columbia, Kelowna, British Columbia, V1V 1V7, Canada*

(Dated: March 30, 2015)

Quantum communication holds the promise of creating disruptive technologies that will play an essential role in future communication networks. For example, the study of quantum communication complexity has shown that quantum communication allows exponential reductions in the information that must be transmitted to solve distributed computational tasks. Recently, protocols that realize this advantage using optical implementations have been proposed. Here we report a proof of concept experimental demonstration of a quantum fingerprinting system that is capable of transmitting less information than the best known classical protocol. Our implementation is based on a modified version of a commercial quantum key distribution system using off-the-shelf optical components over telecom wavelengths, and is practical for messages as large as 100 Mbits, even in the presence of experimental imperfections. Our results provide a first step in the development of experimental quantum communication complexity.

What technological advantages can be achieved by directly harnessing the quantum-mechanical properties of physical systems? In the context of communications, it is known that quantum mechanics enables several remarkable improvements [1, 2]. And yet, despite our advanced understanding of what these quantum advantages are, demonstrating them in a practical setting continues to be an outstanding and central challenge. Important progress has been made in this direction [1], but many cases of quantum improvements have never been realized experimentally.

A particular example of a quantum advantage occurs in the field of communication complexity: the study of the minimum amount of information that must be transmitted in order to solve distributed computational tasks [2]. It has been proven that for certain problems, quantum mechanics allows exponential reductions in communication compared to the classical case. These results, beside being of great fundamental interest, have important practical applications for the design of communication systems, computer circuits, and data structures [2]. However, to date, only a few proof-of-principle implementations of quantum communication complexity protocols have been reported [3–5]. Crucially, none of them have demonstrated a reduction in the transmitted information compared to the classical case.

Recently, protocols have been introduced that are capable of achieving this reduction using practical optical implementations [6, 7], thus opening the door to experimental demonstrations of the exponential reductions of quantum communication complexity. In this work, based on the protocol Ref. [6], we present a proof of concept experimental demonstration of a quantum fingerprinting protocol which is capable of transmitting less information than the best known classical protocol [8].

Quantum fingerprinting: In quantum fingerprinting [9], Alice and Bob are each given an n-bit string, x and y respectively. In the simultaneous message passing model [10], they must each send a message to a third party, the referee, whose task is to decide whether the inputs x and y are equal or not with an error probability of at most ϵ. Alice and Bob do not have access to shared randomness and there is only one-way communication to the referee. In this case, it has been proven that any classical protocol for this problem must transmit at least $\Omega(\sqrt{n})$ bits of information to the referee [11]. On the other hand, a quantum protocol was specified in Ref. [9] that transmits only $O(\log_2 n)$ qubits of information – an *exponential* improvement over the classical case.

Ref. [6] proposed a quantum fingerprinting protocol with weak coherent states. In this protocol, portrayed in Fig. 1, Alice first applies an error-correcting code $E : \{0,1\}^n \to \{0,1\}^m$ to her input x of n bits. This results in a codeword $E(x)$ of m bits, which she uses to prepare a sequence of m coherent states. This sequence of coherent states is given by the state

$$|\alpha, x\rangle = \bigotimes_{i=1}^{m} \left| (-1)^{E(x)_i} \frac{\alpha}{\sqrt{m}} \right\rangle_i .$$

Here $E(x)_i$ is the ith bit of the codeword, α is a complex amplitude and $\mu := |\alpha|^2$ is the total mean photon number in the entire sequence.

Bob does the same as Alice for his input y, and they both send their sequence of states to the referee, who interferes the individual states in a balanced beam-splitter. The referee checks for clicks at the outputs of the interferometer using single-photon detectors, which we label "D_0" and

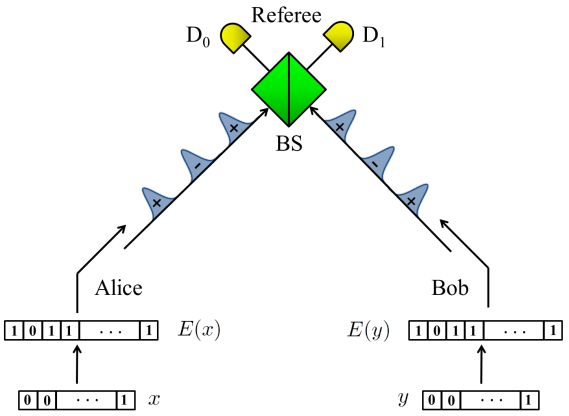

FIG. 1: (Colour online) A schematic illustration of the quantum fingerprinting protocol with coherent states. Alice and Bob receive inputs x and y, respectively, which they feed to an error-correcting code to produce the codewords $E(x)$ and $E(y)$. Using these codewords, they modulate the phases of a sequence of coherent pulses that they send to the referee. The incoming signals interfere at a beamsplitter (BS) and photons are detected in the output using single-photon detectors D_0 and D_1. In an ideal implementation, detector D_1 fires only when the inputs to Alice and Bob are different.

"D_1". In the ideal case, a click in detector D_1 will never happen if the phases of the incoming states are equal, i.e. if $E(x)_i \oplus E(y)_i = 0$. However, it is possible for a click in detector D_1 to occur if the phases are different, i.e. if $E(x)_i \oplus E(y)_i = 1$. Thus, if $x \neq y$, we expect a number of clicks in D_1 that is proportional to the total mean number of photons and the Hamming distance between the codewords. This allows the referee to distinguish between equal and different inputs by simply checking for clicks in detector D_1.

In Ref. [6], it was proven that the maximum quantum information Q that can be transmitted with the states of this protocol satisfies

$$Q = O(\mu \log_2 n),$$

which, for fixed μ, is an exponential improvement over the classical case.

Theoretical contributions: Although the protocol of Ref. [6] is already practical, we overcome various theoretical challenges to enable the protocol to be demonstrated using commercial off-the-shelf components:

1. We develop an efficient error-correction algorithm that allows us to substantially relax the requirements on the experimental devices. Ref. [6] used Justesen codes as an example to illustrate the properties of the protocol. However, these codes are not optimal for quantum fingerprinting. In contrast, we construct a more efficient code based on random Toeplitz matrices. For various rates, our code achieves a minimum distance that is more than three times the value for Justesen codes.

2. We use an improved decision rule for the referee compared to the one used in Ref. [6], which makes the protocol more robust to experimental imperfections.

3. We perform detailed simulations of the protocol that allow us to identify the optimal parameters for performing the experiment.

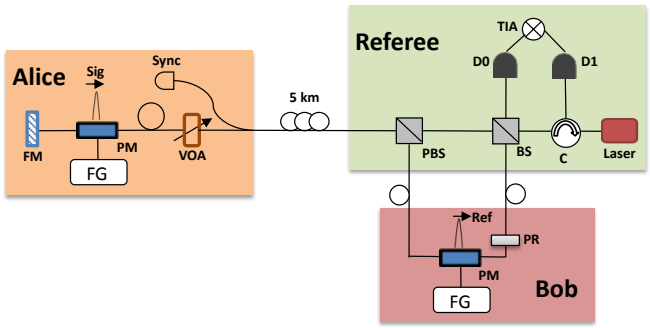

FIG. 2: (Color online) Experimental setup. The laser source at the referee emits photon pulses which are separated at a 50:50 beamsplitter (BS) into two pulses, the signal pulse (Sig) and the reference pulse (Ref). Ref passes through a polarization rotator (PR) and Bob's phase modulator (PM). The pulses are then recombined at a polarization beam splitter (PBS) where they exit through the same port and travel to Alice through the 5 kms fiber. Alice uses the Ref as a synchronization (Sync) and uses her PM to set the phase of Sig according to $E(x)$. Once the two pulses are reflected back by the Faraday mirror (FM), she attenuates them to the desired photon level by using the variable optical attenuator (VOA). When the two pulses return, because of Alice's FM, the Ref will travel through Bob, who uses his PM to modulate the pulse according to $E(y)$. Both Alice and Bob use two external function generators (FG) to control the PMs. Finally, the two pulses arrive simultaneously at the BS, where they interfere and are detected by two detectors D_0 and D_1. The detection events are recorded by a time interval analyzer (TIA).

Experimental demonstration: We implemented the protocol by using a commercial plug&play system originally designed for quantum key distribution (QKD), to which we added several important modifications. Our set-up is shown in Fig. 2. The advantage of the plug&play system is that it offers a particularly robust and stable implementation. We implement the protocol on top of two commercial systems, namely ID-500 and Clavis2, manufactured by ID Quantique [12]. Since the operating conditions of our protocol are significantly different from those of standard QKD, using a commercial QKD equipment for our implementation requires several important modifications to the system:

1. Two single-photon detectors with low dark count rates were installed. Fortunately, our error correction codes improve the tolerance of the protocol to dark counts, which permits us to use commercial detectors. We employ two commercial free-running InGaAs avalanche photodiodes – ID220 [12], and the detection counts are recorded by a time interval analyzer (PicoQuant HydraHarp 400).

2. We use the VOA inside Alice to reduce the mean photon

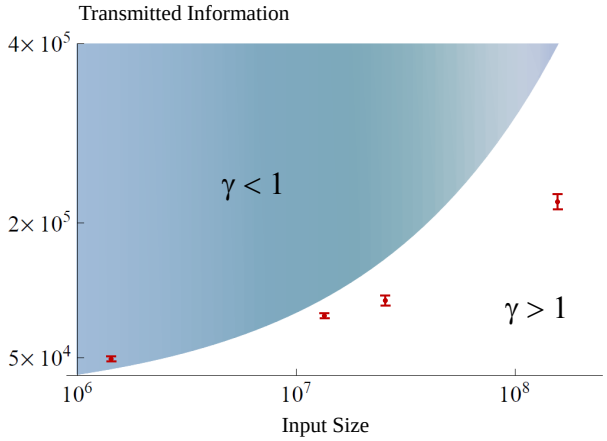

FIG. 3: (Color online) Transmitted information in our protocol. The blue area indicates the region where the classical protocol transmits less information than our protocol, while the red point shows our experimental results. The error bars correspond to one standard deviation. For large n, our results are strictly better than the best known classical protocol for a range of practical values of the input size.

number per pulse down to suitable numbers. These values – in the order of 10^{-5} per pulse – were in fact four orders of magnitude lower than those typically used for QKD. Hence, several calibration processes of the system are required, which imposes particular care in the synchronization of the phase modulation and attenuation signals.

3. Commercial QKD systems like Clavis2 have an internal random number generator to set the phase modulations, which does not allow us to modulate the phases according to the pre-generated codewords. We solve this difficulty by using two external function generators (FG, Agilent 88250A) loaded with the codewords to control Alice's and Bob's PM. This requires precise synchronization and calibration procedures to guarantee correct phase modulations.

All the above modifications led to the development of a practical system that is capable of performing quantum fingerprinting.

Experimental results: We perform the quantum fingerprinting experiment over a standard telecom fiber of 5 km between Alice and the referee. The channel between Bob and the referee is a few meters long. The quantum fingerprinting protocol is tested over several values of the input size n. In Fig. 3, we show the transmitted information as a function of n for a target error probability of $\epsilon = 5 \times 10^{-5}$. The blue area indicates the information transmitted by the best known classical protocol of Ref. [11] which for this probability of error requires the transmission of $16\sqrt{n}$ bits. The red points show our experimental results, where the data point for the largest n is obtained from ID-500 and the other three data points are obtained from Clavis2. The error bars come from the uncertainty in the estimation of the mean photon number μ. For large n, our experimental results are strictly better than those of the classical protocol for a wide range of practical values of the input size. Specifically, the ratio between the transmitted classical information of the best-known classical protocol [11] and the upper bound on the transmitted quantum information is well above 1, and the classical protocol transmitted as much as 66% more information than the quantum protocol.

Conclusion: Based on the protocol of Ref. [6], we have experimentally demonstrated a proof of concept quantum fingerprinting system that is capable of transmitting less information than the best known classical protocol. Our experimental test of this system indicates that its operation is consistent with our model of the devices and hence also with achieving the desired error probability. Moreover, we have operated our system in a parameter regime in which the information transmitted in the protocol is up to 66% lower than the best known classical protocol. This constitutes the first time that a quantum fingerprinting protocol has been carried out that is capable of achieving this reduction in the transmitted information. **More details of our work can be found in the preprint article of Ref. [8].**

---

* These authors contributed equally to this work.
† F. Xu's current address: Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

[1] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014).
[2] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[3] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders, Phys. Rev. Lett. **95**, 150502 (2005).
[4] J. Du, P. Zou, X. Peng, D. K. Oi, L. Kwek, C. Oh, and A. Ekert, Phys. Rev. A **74**, 042319 (2006).
[5] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Zukowski, and H. Weinfurter, Phys. Rev. A **72**, 050305 (2005).
[6] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).
[7] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **90**, 042335 (2014).
[8] F. Xu, J. M. Arrazola, et al., arXiv preprint arXiv:1503.05499 (2015).
[9] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[10] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (1979), pp. 209–213.
[11] L. Babai and P. G. Kimmel, in *Proceedings of the 12th Annual IEEE Conference on Computational Complexity* (IEEE, IEE, Los Alamitos, California, 1997), pp. 239–246.
[12] IDQuantique, Geneva, http://www.idquantique.com.