Observation of quantum fingerprinting beating the classical limit

Jian-Yu Guan,[1,2] Feihu Xu,[3,*] Hua-Lei Yin,[1,2] Yuan Li,[1,2] Wei-Jun Zhang,[4] Si-Jing Chen,[4] Xiao-Yan Yang,[4] Li Li,[1,2] Li-Xing You,[4] Teng-Yun Chen,[1,2] Zhen Wang,[4] Qiang Zhang,[1,2,5] and Jian-Wei Pan[1,2]

[1]*Department of Modern Physics and National Laboratory for Physical Sciences at Microscale,*
Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China
[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics,*
Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China
[3]*Research Laboratory of Electronics, Massachusetts Institute of Technology,*
77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA
[4]*State Key Laboratory of Functional Materials for Informatics,*
Shanghai Institute of Microsystem and Information Technology,
Chinese Academy of Sciences, Shanghai200050, China
[5]*Jinan Institute of Quantum Technology, Jinan, Shandong, 250101, China*

Quantum communication promises the remarkable advantage of an exponential reduction in the transmitted information over classical communication to accomplish distributed computational tasks. However, to date, demonstrating this advantage in a practical setting continues to be a central challenge. Here, we report an experimental demonstration of a quantum fingerprinting protocol that for the first time surpasses the ultimate classical limit to transmitted information. Ultra-low noise superconducting single-photon detectors and a stable fibre-based Sagnac interferometer are used to implement a quantum fingerprinting system that is capable of transmitting less information than the classical proven lower bound over 20 km standard telecom fibre for input sizes of up 2 Gbits. The results pave the way for experimentally exploring the advanced features of quantum communication and open a new window of opportunity for research in communication complexity.

In quantum communication, so far, only one protocol – quantum key distribution (QKD) – has been widely investigated and deployed in commercial applications. It is thus highly important to exploit the practically available quantum communication protocols beyond QKD in order to fully understand the potential of large-scale quantum communication networks. Despite significant progress in this direction [1], the rich class of quantum communication complexity (QCC) protocols [2, 3] remains largely undemonstrated, except for a few proof-of-principle implementations [4–7]. The field of QCC explores quantum-mechanical properties in order to determine the minimum amount of information that must be transmitted to solve distributed computational tasks [3]. It not only has many connections to the foundational issues of quantum mechanics, but also has important applications for the design of communication systems, green communication techniques, computer circuits and data structures.

Quantum fingerprinting, proposed by Buhrman, Cleve, Watrous and Wolf, is the most appealing protocol in QCC [8]. Specifically, the simultaneous message-passing model [2] corresponds to the scenario where two parties, Alice and Bob, respectively receive inputs $x_a, x_b \in \{0,1\}^n$ and send messages to a third party, Referee, who must determine whether x_a equals x_b or not, with a small error probability ϵ. This model has two requirements: (i) Alice and Bob do *not* have access to shared randomness; (ii) there is one-way communication to Referee *only*. Alice and Bob can achieve their goal by sending *fingerprints* of their original inputs that are much shorter than the original inputs. It has been shown that the optimal classical protocols require fingerprints of a length that is at least $\mathcal{O}(\sqrt{n})$ [9], while, using quantum communication, Alice and Bob need to send fingerprints of only $\mathcal{O}(\log n)$ qubits [8]. Therefore, when the goal is to reduce the transmitted information, quantum communication provides an exponential improvement over the classical case. Despite this advantage, demonstrating it in a practical setting continues to be a challenge [4–6].

Recently, a coherent-state quantum fingerprinting protocol for the realization with linear optics and without entangled states was proposed by Arrazola and Lütkenhaus [10]. On the basis of this protocol, Xu *et al.* reported a proof-of-concept implementation that transmits less information than the best known classical protocol [7]. Nonetheless, as noted already in ref. [7], a remaining question is “whether quantum fingerprinting can beat the classical theoretical limit of transmitted information." This limit has been proven to be roughly two orders of magnitude smaller than the best known classical protocol [9], and surpassing it has been a long-standing experimental challenge. In this work, a quantum fingerprinting system is designed and demonstrated that for the first time beats the classical limit to transmitted information by up to 84%.

The experiment adopted the coherent-state quantum fingerprinting protocol [10]. In this protocol, Alice applies an error-correcting code (ECC) to her input x_a of n bits and generates a codeword $E(x_a)$ of $m = n/R$ bits (with R indicating the rate of ECC). Then she prepares a

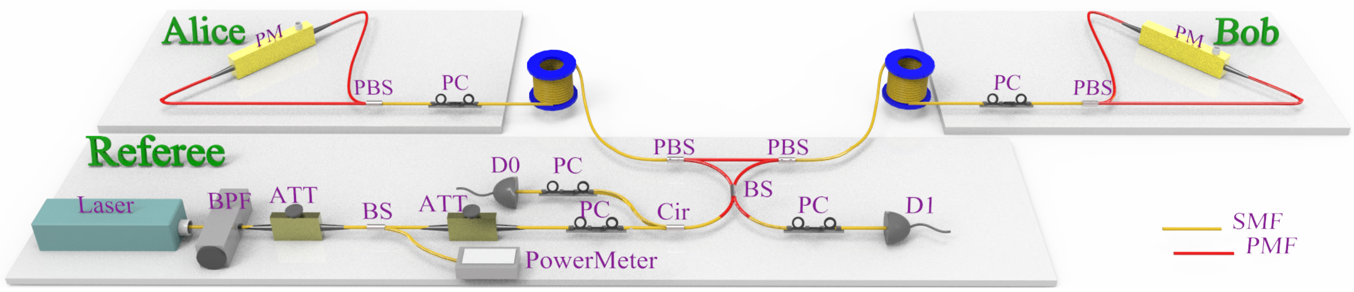

FIG. 1: Experimental set-up of the quantum fingerprinting. PM: phase modulator. BS: beam splitter. BPF: bandpass filter. ATT: attenuator. PC: polarization controller. Cir: circulator. PBS: polarization beam splitter. PMF: polarization maintaining fibre. SMF: standard single mode fibre. D_0/D_1: superconducting single-photon detector.

sequence of m weak coherent pulses and uses the codeword to modulate the phase of each pulse. 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 "D_1". In the ideal case, a click in detector D_1 will never happen if the phases of the incoming pulses are equal. However, it is possible for a click in detector D_1 to occur if the phases are different. 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 [7].

In Ref. [10], it was proven that the maximum quantum information Q that can be transmitted with the states of this protocol satisfies

$$Q = O(\mu \log_2 n), \tag{1}$$

where μ is defined as the total mean photon number in the entire pulse sequence. An important feature of the protocol is to fix μ to a small constant. For a fixed μ, Q corresponds to an exponential improvement over the classical case of $\mathcal{O}(\sqrt{n})$ bits [9], which precisely provides the quantum advantage.

To implement the protocol, the experiment utilizes a fibre-based Sagnac-type interferometer, as sketched in Fig. 1. In this set-up, the referee sends a weak coherent pulse at 1532 nm and splits the pulse into two pulses – left pulse and right pulse – by a beam splitter (BS) at his output. Once the left pulse reaches Alice after the transmission over a fiber spool, she performs a polarization compensation without any phase modulation and then guides the pulse back to the referee. Due to the polarization rotation at Alice, this pulse will travel to Bob, who conducts the phase modulation by using his phase modulator (PM) according to his codeword $E(x_b)$. The same process applies to the right pulse, which first goes to Bob and then undergoes the encoding by Alice according to the codeword $E(x_a)$. Finally, once the two pulses return to the referee, they interfere at the referee's BS and the detection events are registered using two high-quality superconducting nanowire single photon detectors (SNSPDs). Since the two pulses, sent from Referee to Alice and Bob, travel exactly the same path in the interferometer, two remarkable features are automatic compensation of the phase differences between the two pulses and high interference visibility. Indeed, the monitored stability of the system is that the interference visibility remains over 96% during 24 hours of continuous operation.

In experiment, one challenge is that the coherent-state quantum fingerprinting protocol [10] requires the operation of the system at an ultra-low mean photon number, which is well below 10^{-7} per pulse. Indeed, as can be deduced from Eq. (1), a lower mean photon number leads to a reduction in the transmitted information, which permits the demonstration of beating the classical limit. To properly detect such a weak signal, advanced SNSPDs with on-chip narrow-band-pass filters [11] are installed. These SNSPDs have an *ultra-low* dark count rate of about 0.11 Hz and a high quantum efficiency of 45.6% at 1532nm wavelength.

To surpass the classical limit, the losses should be carefully controlled. The overall transmittance of Referee's PBS and BS is 80.16% (78.5%) from Alice (Bob) to Referee. The system is implemented with total distances (from Alice to Bob) of 0 km, 10 km and 20 km fibre spools, whose losses are characterised to be about 0 dB, 1.86 dB and 3.92 dB respectively. Under each distance, five different message sizes n, up to 2 Gbits, are chosen. The experimental results are shown in Fig. 2.

Fig. 2a shows the experimental transmitted information for different message sizes. The error bars come from the uncertainty in the estimation of the mean photon number μ. The best known classical protocol needs to transmit at least $32\sqrt{n}$ bits of information [9]. On the basis of the references [9], we prove an optimized bound

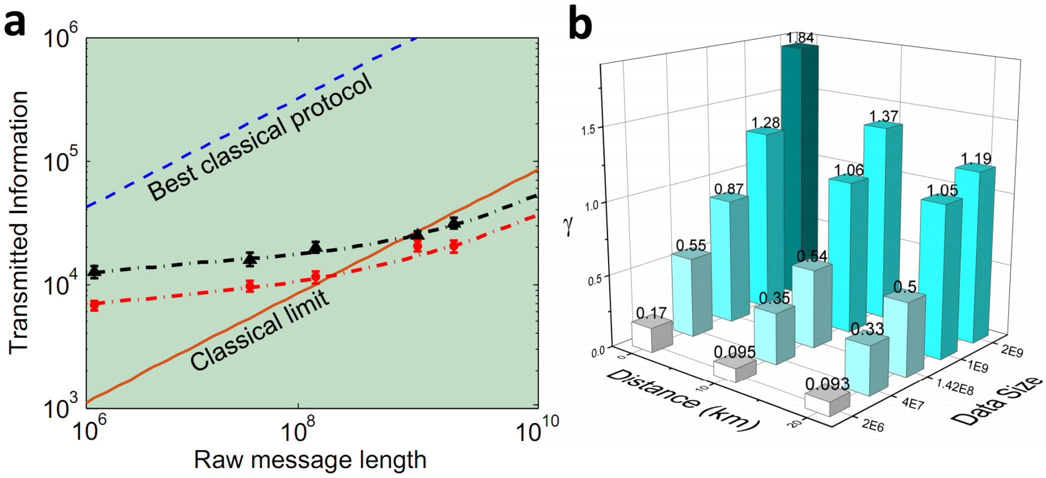

FIG. 2: (Color online) **a,** Log-log plot of the total transmitted information. The red and black points are the experimental results at 0 km and 20 km respectively. For large n, our results are, in strict terms, better than the classical limit for a wide range of practical values of the input size. **b,** The ratio γ between classical limit C_{limit} and the transmitted quantum information Q. For the three small input sizes, no advantage over the classical limit was obtained. However, for the two large input sizes, the ratio is well above one over different fibre distances.

for the classical limit. This bound is given by

$$C_{\text{limit}} = (1 - 2\sqrt{\epsilon})\sqrt{\frac{n}{2\ln 2}} - 1. \qquad (2)$$

Fig. 2a indicates that, with the increase of input size n, the classical limit scales linearly in the log-log plot, while the transmitted quantum information remains almost a constant. The transmitted information is up to two orders of magnitude lower than that in the previous experiment [7]. Importantly, for large n, these experimental results clearly beat the classical limit for a wide range of practical values of the input size.

To further illustrate our results, γ is defined as the ratio between the classical limit C_{limit} and the transmitted quantum information Q, i.e., $\gamma = C_{\text{limit}}/Q$. A value $\gamma > 1$ implies that the classical limit is surpassed by our quantum fingerprinting protocol. In Fig. 2b, γ is plotted as a function of different fibre distances and input data sizes. For the input sizes larger than one Gbit, γ is well above one. The ratio is as large as $\gamma = 1.84$, which implies that our quantum fingerprinting implementation beats the classical limit by up to 84%.

Finally, to show the ability of the quantum protocol in the real world, two video files with sizes of two Gbits were experimentally fingerprinted over 20 km fibre. A 14% reduction in the transmitted information was obtained, as compared to the classical limit.

To conclude, by using ultra-low dark count superconducting detectors (i.e., ∼0.1 Hz), as well as an automatic-phase compensation Sagnac system, a quantum-enhanced method for fingerprinting to beat the ultimate classical theoretical limit was demonstrated. Since quantum communication complexity is intimately linked to several foundational issues of quantum mechanics [3], our experiment provides a first step in the development of experimental quantum communication complexity, which could even lead new proposals for experiments that test the foundations of physics.

More details of our work can be found in the preprint article of [Guan et al., arXiv:1603.02089 (2016)].

[*] Electronic address: fhxu@mit.edu

[1] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014).

[2] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (1979), pp. 209–213.

[3] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).

[4] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Zukowski, and H. Weinfurter, Phys. Rev. A **72**, 050305 (2005).

[5] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders, Phys. Rev. Lett. **95**, 150502 (2005).

[6] J. Du, P. Zou, X. Peng, D. K. Oi, L. Kwek, C. Oh, and A. Ekert, Phys. Rev. A **74**, 042319 (2006).

[7] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus, and H.-K. Lo, Nature communications **6**, 8735 (2015).

[8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[9] 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.

[10] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).

[11] X. Yang, H. Li, L. You, W. Zhang, L. Zhang, Z. Wang, and X. Xie, Applied optics **54**, 96 (2015).