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, Shanghai 200050, China*

[5]*Jinan Institute of Quantum Technology, Jinan, Shandong, 250101, China*

(Received 19 March 2016; published 13 June 2016)

Quantum communication has historically been at the forefront of advancements, from fundamental tests of quantum physics to utilizing the quantum-mechanical properties of physical systems for practical applications. In the field of communication complexity, quantum communication allows the 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 a proof-of-principle experimental demonstration of a quantum fingerprinting protocol that for the first time surpasses the ultimate classical limit to transmitted information. Ultralow noise superconducting single-photon detectors and a stable fiber-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 fiber for input sizes of up to 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 and testing the foundations of physics.

DOI: 10.1103/PhysRevLett.116.240502

The quantum-communication network [1] is believed to be the next-generation platform for remote information processing tasks. So far, however, only one protocol—quantum key distribution (QKD) [2,3]—has been widely investigated and deployed in commercial applications. The extension of the practically available quantum communication protocols beyond QKD in order to fully understand the potential of large-scale quantum communication networks is therefore highly important. Significant progress has been made in this direction [4–9], but the rich class of quantum communication complexity (QCC) protocols [10–12] remains largely undemonstrated, except for a few proof-of-principle implementations [13–16]. 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 [11]. It not only has many connections to the foundational issues of quantum mechanics [12,17], but also has important applications for the design of communication systems, green communication techniques, computer circuits, and data structures [18]. For instance, QCC essentially connects the foundational physics questions regarding nonlocality with those of communication complexity studied in theoretical computer science [12].

Quantum fingerprinting, proposed by Buhrman, Cleve, Watrous, and Wolf, is the most appealing protocol in QCC [19]. Specifically, the simultaneous message-passing model [10] 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 $\mathcal{O}(\sqrt{n})$ [20,21], while, using quantum communication, Alice and Bob need to send fingerprints of only $\mathcal{O}(\log n)$ qubits [19,22]. 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 [12].

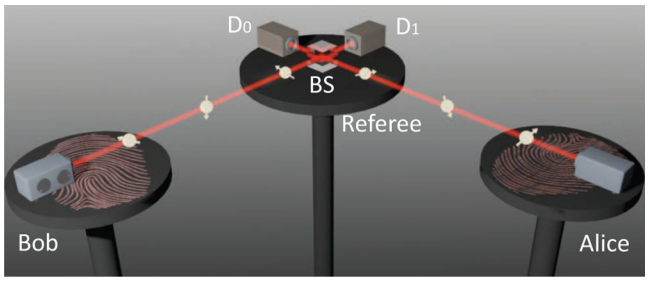

FIG. 1. A schematic illustration of the coherent-state quantum fingerprinting protocol. Alice and Bob use their input digital bits to modulate the phases of a sequence of weak coherent pulses and they send the sequence to Referee over two quantum channels. The incoming signals interfere at a beam splitter (BS), and photons are detected in the output by two detectors D_0 and D_1.

References [14,15] have reported heroic attempts at implementing quantum fingerprinting, but a drawback is that their fingerprint states must be highly entangled. Recently, a coherent-state quantum fingerprinting protocol for the realization with linear optics and without entangled states was proposed by Arrazola and Lütkenhaus [23]. 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 [16]. Nonetheless, as noted already in Ref. [16], a remaining question is "whether quantum fingerprinting can beat the classical theoretical limit of transmitted information." This limit has been proven to be roughly 2 orders of magnitude smaller than the best known classical protocol [21], and surpassing it has been a long-standing experimental challenge. In this work, a proof-of-principle quantum fingerprinting system is designed and demonstrated, which, for the first time, beats the classical limit to transmitted information by up to 84%.

As illustrated in Fig. 1, the experiment adopted the coherent-state quantum fingerprinting protocol [23]. The detailed description of the protocol is presented.

(i) Preparation.—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 sequence of m weak coherent pulses and uses the codeword to modulate the phase of each pulse. The sequence of coherent states can be understood as a coherent version of the encoding of a single photon across m modes. Bob completes a process that is the same as Alice's for his input x_b.

(ii) Distribution.—Both Alice and Bob send their pulse trains to the Referee over two quantum channels. By using a phase interferometer, Referee interferes the individual pulses in a balanced beam splitter and observes the clicks at the outputs of the BS, using two single-photon detectors, which are labeled "D_0" and "D_1." This process allows Referee to verify whether the relative phases of the incoming pulses are the same or different [24]. In an ideal situation, a click in detector D_1 will never happen if the phases of the pulses are equal.

(iii) Decision.—In the presence of experimental imperfections such as detector dark counts and imperfect interference, detector D_1 may fire even when the inputs are equal. However, in a case of small imperfections, the total number of clicks on D_1 for different inputs is much larger than the total number of clicks for equal inputs. A decision rule for Referee is employed on the basis of only the total number of clicks observed in detector D_1 [16]. Referee sets a threshold value $D_{1,\mathrm{th}}$ such that, if the number of clicks is smaller than or equal to $D_{1,\mathrm{th}}$, he will conclude that the inputs are equal. Otherwise, he concludes that they are different. In the protocol, the value of $D_{1,\mathrm{th}}$ is chosen in such a way that an error is equally likely to occur for equal and unequal inputs.

It has been proven that the quantum information Q that can be transmitted by sending the sequence of weak coherent states satisfies [23]

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

where μ is defined as the *total* mean photon number in the entire pulse sequence sent by both Alice and Bob. An important feature of the protocol is to fix μ to a small constant [25], and for a fixed μ, Q corresponds to an exponential improvement over the classical case of $\mathcal{O}(\sqrt{n})$ bits [20,21]. It is precisely in terms of this reduction in the transmitted information that the quantum protocol provides an advantage over the classical case [23].

To implement the coherent-state quantum fingerprinting protocol, the experiment utilizes a fiber-based Sagnac-type interferometer, as sketched in Fig. 2. In this setup, the referee sends a 1532 nm weak coherent pulse at 25 MHz and splits the pulse into two pulses—left pulse and right pulse—by a beam splitter 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. Because of 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). In front of each SNSPD, a polarization controller (PC) is used to optimize the detection efficiency. See Ref. [26] for the experimental details.

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

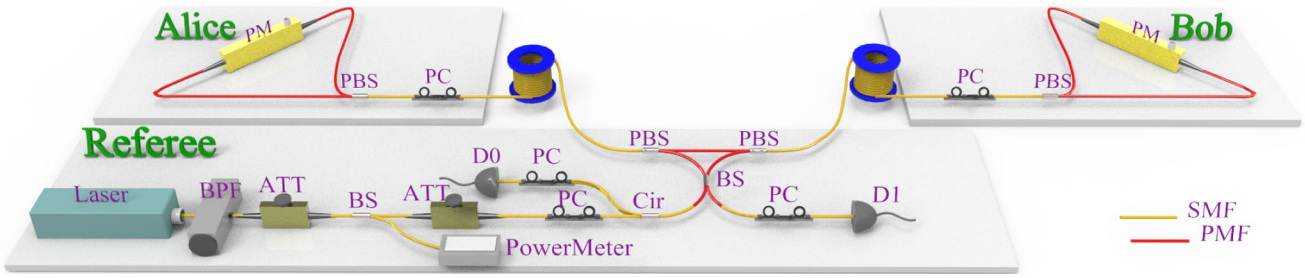

FIG. 2. Experimental setup of the quantum fingerprinting. Referee sends weak coherent pulses to Alice and Bob, who encode the phase of each of the pulses, using their phase modulator (PM) according to their codewords. The encoded pulses return and arrive simultaneously at Referee's input beam splitter, where they interfere and are finally detected by two superconducting single-photon detectors (D_0 and D_1). BPF, bandpass filter; ATT, attenuator; PC, polarization controller; Cir, circulator; PBS, polarization beam splitter; PMF, polarization maintaining fiber; SMF, standard single mode fiber.

visibility. Note that the Sagnac configuration guarantees the phase stability between Alice and Bob, but with the price of redundant transmission for each pulse. In experiment, one challenge is that Alice (Bob) should ensure that her (his) PM modulates *only* the signal pulse, i.e., the one that returns from Bob (Alice), instead of the compensation pulse, i.e., the pulse that is sent directly from Referee. To do so, specific lengths of fibers and electrical cables are designed to separate the signal pulse from the compensation pulse with 20 ns difference, and to carefully control the electrical gating signals applied to the PMs. Another challenge is that the coherent-state quantum fingerprinting protocol [23] requires the operation of the system at an ultralow mean photon number per pulse $\mu_{\text{pulse}} = (\mu/2m)$, which is well below 10^{-7}. 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 [31,32] are installed. These SNSPDs have an *ultralow* dark count rate of about 0.11 Hz and a high quantum efficiency of 45.6% at 1532 nm wavelength.

To surpass the classical limit, the losses should be carefully controlled. When light travels back from Alice (Bob) to Referee, the total loss of Referees PBS and BS is 0.96 dB (1.05 dB). The system is implemented with total distances (from Alice to Bob) of 0, 10, and 20 km fiber spools, whose losses are characterized to be about 0, 1.86, and 3.92 dB, respectively [33]. Under each distance, five different message sizes n are chosen as 2×10^6, 4×10^7, 1.42×10^8, 1×10^9, and 2×10^9. For each message, an ECC is applied based on the Toeplitz-matrices random linear code [16], which has a rate of $R = 0.24$ and a minimum distance of $\delta = 0.22$. The random numbers to construct the matrices are generated from a quantum random number generator [34].

A stable interference is important to run different input sizes. The stability of the system is monitored, and the result is that, during 24 hours of continuous operation, the overall intensity fluctuations are less than 3.7% and the interference visibility remains over 96%. In the experiment, the key observation parameter is the number of counts on detector D_1. These experimental results are shown in Fig. 3. The clear difference between the worst-case different inputs with $\delta = 0.22$ difference (blue points) and the identical inputs (red points) makes it possible to run the protocol. In all the runs of experiments, a maximal error probability of $\epsilon = 2.6 \times 10^{-5}$ [26] was achieved. The maximum error probability was calculated from the theoretical model of the experiment [16,23]. We remark that to fingerprint two 2 Gbits messages over 20 km, our system requires a communication time of ~5.6 min [35], while it transmits only a total number of $\mu = 1250$ photons, i.e., $\mu_{\text{pulse}} = 0.8 \times 10^{-7}$.

Figure 4(a) shows the experimental transmitted information at 0 km (red data points) and 20 km (black data points) for different message sizes. The error bars come from the uncertainty in the estimation of the mean photon number μ. In this figure, our quantum fingerprinting is compared with the classical limit (solid-orange curve) and the best known classical protocol (dashed-blue curve). The best known classical protocol needs to transmit at least $32\sqrt{n}$ bits of information [21]. On the basis of Refs. [20,21], we prove an optimized bound for the classical limit [36]. This bound is given by [26]

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

Figure 4(a) 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 2 orders of magnitude lower than that in the previous experiment [16]. 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

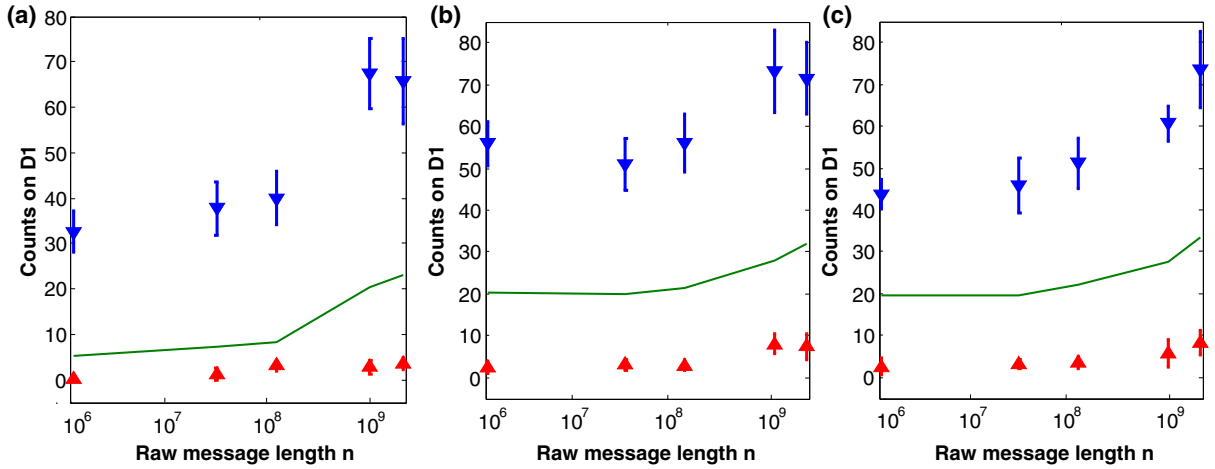

FIG. 3. The experimental counts on D_1 for (a) 0, (b) 10, and (c) 20 km. The blue points indicate the counts for two messages with $\delta = 0.22$ difference, while the red points show the counts for two identical messages. The green curve is the threshold value $D_{1,\mathrm{th}}$. The error bars correspond to 1standard deviation, which is quantified by repeating the experiment 10 times.

our quantum fingerprinting protocol. In Fig. 4(b), γ is plotted as a function of different fiber distances and input data sizes. For the input sizes larger than 1 Gbit, γ is well above 1. The ratio is as large as $\gamma = 1.84$, which implies that our quantum fingerprinting implementation beats the classical limit by up to 84%.

To show the ability of the quantum protocol in the real world, two video files with sizes of 2 Gbits [37] were experimentally fingerprinted over 20 km fiber by using ~1300 transmitted photons as the information carrier. A 14% reduction in the transmitted information was obtained, as compared to the classical limit [26], and the potential for practical applications was thus indicated.

Finally, we discuss the limitations of our experiment and possible solutions. First, from a practical perspective, the required number of pulses or experimental communication time evolves linearly with the input size n, which is quadratically larger than in the classical case [16,23]. However, the number of photons used in experiment $[O(1)]$ is more than quadratically smaller than in a classical implementation $[O(\sqrt{n})]$. Therefore, if running time during communication is *a priority*, our experiment has a disadvantage. Nonetheless, if minimizing energy expenditures is *a priority*, our experiment offers a significant advantage. Second, with the increase of the channel distance, the current system requires transmitting more photons to compensate the channel loss and the interference visibility also decreases, which in turn diminishes the advantage of suppressing the classical limit. However, this can be improved by using higher detection efficiency SNSPDs [38] and better thermoinsulated and vibration-isolated material. Third, there is a direct connection between Alice and Bob in our system configuration, which makes it difficult in practice to guarantee the assumption that Alice

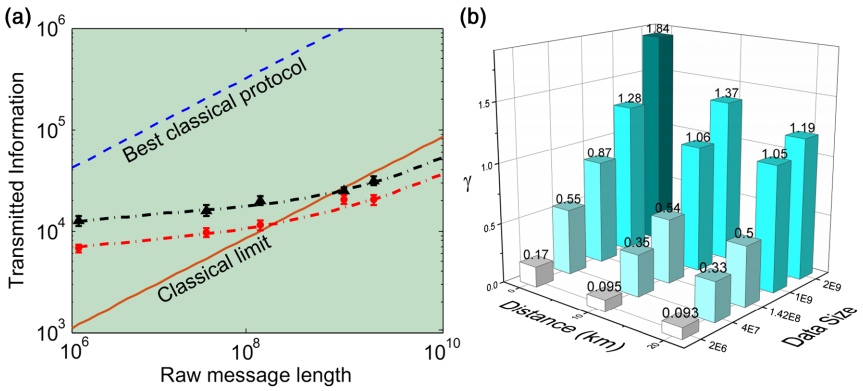

FIG. 4. (a) Log-log plot of the total transmitted information. The red and black points are the experimental results at 0 and 20 km, respectively. For various n, the transmitted information of our experimental quantum fingerprinting protocol is much lower than the transmitted information of the best known classical algorithm. 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 1 over different fiber distances. Our experiment transmitted as much as 84% less information than the classical limit.

and Bob cannot share randomness. This can be improved by the scheme that Alice and Bob hold independent laser sources, but with the price of complex phase-locking techniques to interfere the pulses. Last, but not least, all electrical synchronization is local, but distributed synchronization can be realized by using the technique developed recently in QKD [39]. This enables the demonstration in the metropolitan fiber network for a field test.

Overall, by using ultralow dark count superconducting detectors (i.e., ~0.1 Hz) and 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 [12], 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.

The authors thank J. M. Arrazola, N. Lütkenhaus, H.-K. Lo, X. Xie, and M. Jiang for valuable discussions. Particularly, we thank Mike W. Wang for his help on the plot of Fig. 1 and the implementation of ECC. This work was supported by the National Fundamental Research Program (under Grants No. 2011CB921300 and No. 2013CB336800), the National Natural Science Foundation of China, the Chinese Academy of Science, the 10000-Plan of Shandong Province, the Management Committee of Shanghai Zhangjiang High-Technology Industrial Development Zone. F. Xu acknowledges the support from the Office of Naval Research (ONR) and the Air Force Office of Scientific Research (AFOSR).

J.-Y. G., F. X., and H.-L. Y. contributed equally to this work.

Note added—Recently, we became aware that a similar optimized classical lower bound has been proved independently by [36].

*eidos@ustc.edu.cn
†lxyou@mail.sim.ac.cn
‡qiangzh@ustc.edu.cn
§pan@ustc.edu.cn

[1] J. Qiu, Nature (London) **508**, 441 (2014).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[4] G. Berlín, G. Brassard, F. Bussiéres, N. Godbout, J. A. Slater, and W. Tittel, Nat. Commun. **2**, 561 (2011).
[5] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nat. Commun. **3**, 1326 (2012).
[6] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[7] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **111**, 180504 (2013).
[8] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li *et al.*, Phys. Rev. Lett. **112**, 010504 (2014).
[9] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nat. Commun. **5**, 3717 (2014).
[10] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery (ACM), New York, 1979), p. 209.
[11] G. Brassard, Found. Phys. **33**, 1593 (2003).
[12] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[13] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Zukowski, and H. Weinfurter, Phys. Rev. A **72**, 050305 (2005).
[14] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders, Phys. Rev. Lett. **95**, 150502 (2005).
[15] J. Du, P. Zou, X. Peng, D. K. L. Oi, L. C. Kwek, C. H. Oh, and A. Ekert, Phys. Rev. A **74**, 042319 (2006).
[16] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus, and H.-K. Lo, Nat. Commun. **6**, 8735 (2015).
[17] A. M. Steane and W. van Dam, Phys. Today **53**, No. 2, 35 (2000).
[18] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, England, 2006).
[19] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[20] I. Newman and M. Szegedy, in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery (ACM), New York, 1996), p. 561.
[21] L. Babai and P. G. Kimmel, in *Proceedings of the 12th Annual IEEE Conference on Computational Complexity* (IEEE, IEE, Los Alamitos, CA, 1997), p. 239.
[22] S. Massar, Phys. Rev. A **71**, 012310 (2005).
[23] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).
[24] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[25] By doing so, we are restricting ourselves to an exponentially small subspace of the larger Hilbert space associated with the optical modes. This in turn restricts the capability of these systems to transmit information.
[26] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.116.240502 for the experimental details, the proof of optimized classical bound and the detailed experimental results, which includes Refs. [27–30].
[27] N. Alon and J. H. Spencer, *The Probabilistic Method* (John Wiley & Sons, New York, 2004).
[28] V. Guruswami, A. Rudra, and M. Sudan, Essential coding theory, 2014, http://www. cse. buffalo. edu/atri/courses/coding-theory/book/index. html.
[29] E. N. Gilbert, Bell Syst. Tech. J. **31**, 504 (1952).
[30] R. Varshamov, Dokl. Akad. Nauk SSSR **117**, 739 (1957).

[31] X. Yang, H. Li, W. Zhang, L. You, L. Zhang, X. Liu, Z. Wang, W. Peng, X. Xie, and M. Jiang, Opt. Express **22**, 16267 (2014).
[32] X. Yang, H. Li, L. You, W. Zhang, L. Zhang, Z. Wang, and X. Xie, Appl. Opt. **54**, 96 (2015).
[33] The distances between Alice (or Bob) and the referee are 0 km, 5 km and 10 km.
[34] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).
[35] 2 Gbits message requires the transmission of 8.34 giga-pulses (see Supplement Table 1). Given that the system's pulse repetition rate is 25 MHz, each round of experiment requires $8340/25 = 333.6$ seconds for the transmission of pulses.
[36] D. Touchette, J. M. Arrazola, and N. Lütkenhaus (unpublished).
[37] The two videos can be downloaded from http://news.ustc.edu.cn/images/USTCStory.mp4?download=1 and http://en.ustc.edu.cn/images/USTCStory.mp4?download=1.
[38] F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin *et al.*, Nat. Photonics **7**, 210 (2013).
[39] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).