# Experimental Quantum Randomness Processing Using Superconducting Qubits

Xiao Yuan,[1] Ke Liu,[1] Yuan Xu,[1] Weiting Wang,[1] Yuwei Ma,[1] Fang Zhang,[1] Zhaopeng Yan,[1] R. Vijay,[2] Luyan Sun,[1,*] and Xiongfeng Ma[1,†]

[1]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[2]*Department of Condensed Matter Physics and Materials Science, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400005, India*

(Received 23 February 2016; published 29 June 2016)

Coherently manipulating multipartite quantum correlations leads to remarkable advantages in quantum information processing. A fundamental question is whether such quantum advantages persist only by exploiting multipartite correlations, such as entanglement. Recently, Dale, Jennings, and Rudolph negated the question by showing that a randomness processing, quantum Bernoulli factory, using quantum coherence, is strictly more powerful than the one with classical mechanics. In this Letter, focusing on the same scenario, we propose a theoretical protocol that is classically impossible but can be implemented solely using quantum coherence without entanglement. We demonstrate the protocol by exploiting the high-fidelity quantum state preparation and measurement with a superconducting qubit in the circuit quantum electrodynamics architecture and a nearly quantum-limited parametric amplifier. Our experiment shows the advantage of using quantum coherence of a single qubit for information processing even when multipartite correlation is not present.

DOI: 10.1103/PhysRevLett.117.010502

Coherent superposition of different states, coherence, is a peculiar feature of quantum mechanics that distinguishes itself from Newtonian theory. In different scenarios, coherence exhibits as various quantum resources, such as entanglement [1], discord [2], and single-party coherence [3]. In many quantum information tasks, the common resource leading to quantum advantage is multipartite quantum correlations. For instance, entanglement plays a crucial role in quantum key distribution [4,5], teleportation [6], and computation [7,8]. While the essence of multipartite correlation originates from coherent superposition, it is natural to expect the essence of quantum advantage to also originate from coherence. This raises a fundamental question: Can quantum advantage be obtained without using multipartite correlations?

In randomness generation, it has been shown that coherence is the essential resource for generating true random numbers [9]. It is thus natural to expect coherence to be a resource for displaying quantum advantages in certain randomness related tasks. Remarkably, in a recent work by Dale *et al.*, a rather simple task of randomness processing is proposed to show that coherence yields a provable quantum advantage over classical stochastic physics [10]. In this randomness processing task, a classical coin [see Fig. 1(a)] corresponds to a classical machine that produces independent and identically distributed random variables where each one has the binary values head (0) and tail (1). A coin is called $p$-coin if the probability of producing a head is $p$, where $p \in [0, 1]$. Given an unknown $p$-coin, an interesting question is whether one can construct an $f(p)$-coin, where $f(p)$ is a function of $p$ and $f(p) \in [0, 1]$. Such construction processing is called a Bernoulli factory [11,12].

Let us take $f(p) = 1/2$, for example, which was solved by von Neumann with a rather simple but heuristic strategy [13]. Flip the $p$-coin ($p \neq 0$) twice. If the outcomes are the same, start over; otherwise, output the second coin value as the $1/2$-coin output. Therefore, the function of $f(p) = 1/2$ can be constructed from an arbitrary unknown $p$-coin. As a generalization, a natural question involves which kind of function $f(p)$ can be constructed from an unknown $p$-coin. This classical Bernoulli factory problem was solved by Keane and O'Brien [14]. Generally speaking, a necessary condition for $f(p)$ being constructible is that $f(p) \neq 0$ or 1 when $p \in (0, 1)$. The function $f(p) = 1/2$ satisfies this condition, while there are many other examples that violate it. For instance, surprisingly, the simple "probability amplification" function $f(p) = 2p$ [15] does not satisfy the constructible condition, where we have $f(1/2) = 1$. Therefore, there is no classical method to construct an $f(p) = 2p$-coin.

In the language of quantum mechanics, a $p$-coin corresponds to a machine that outputs identically mixed qubit states,

$$\rho_C = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|, \tag{1}$$

where $p \in [0, 1]$, and $Z = \{|0\rangle, |1\rangle\}$ is the computational basis denoting head and tail, respectively. As $p$ is generally unknown, we can regard $\rho_C$ as a classical way of encoding an unknown parameter $p$. A measurement in the $\{|0\rangle, |1\rangle\}$ basis would output a head or a tail with a probability according to $p$ and $1 - p$, respectively. On the other hand, a quantum way of encoding $p$ [see Fig. 1(b)] can be a coherent superposition of $|0\rangle$ and $|1\rangle$, i.e., $\rho_Q = |p\rangle\langle p|$, with

 

$$|p\rangle = \sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle. \quad (2)$$

Following the nomenclature in Ref. [10], we call such a quantum coin a *quoin*. It is straightforward to see that a $p$-coin can always be constructed from a $p$-quoin by measuring it in the $Z$ (computational) basis. Thus, classically constructible (via coins) $f(p)$ functions are also quantum mechanically constructible (via quoins), while a really interesting question is whether the set of quantum constructible functions (via a quantum Bernoulli factory) is strictly larger than the classical set.

In Ref. [10], Dale *et al.* have theoretically proved the necessary and sufficient conditions for $f(p)$ being quantum constructible. Specifically, they show that there are functions—for instance $f(p) = 2p$—which are impossible to construct classically but can be efficiently realized in the presence of $p$-quoins. Therefore, they provide a positive answer to this problem where quantum resources are strictly superior to classical ones. The protocol for generating the $f(p) = 2p$ function relies on Bell state measurement on two quoins, which essentially establish entanglement between the two quoins.

Now, we are interested in seeing whether such a quantum advantage persists even when multipartite correlations, such as entanglement, are absent. Thus, we only allow single-qubit operations. Without two-qubit operations, it turns out that constructing the $f(p) = 2p$ function will require many copies of qubits defined in Eq. (2), and the convergence could be poor. In this Letter, we propose another function that is impossible with classical means but feasible with only a limited number of single-qubit operations.

*Theoretical protocol.*—In this Letter, we analyze a classically impossible $f(p)$ function defined by

$$f(p) = 4p(1-p). \quad (3)$$

For $p = 1/2$, we have $f(p) = 1$, which means that this function is classically unachievable. On the other hand, it is straightforward to check to see that the $f(p)$ function satisfies the requirements for being quantum constructible [10]. Given a $p$-quoin, we explicitly present an efficient protocol for generating an $f(p)$-coin as shown in Table I.

In our protocol, generating the $q$-coin, where

$$q = -$$

$f(p) = 1$ when $p = 1/2$. Following previous studies [17–19], we employ a truncated function,

$$f_t = \min\{f, 1 - \epsilon\}, \tag{6}$$

with $\epsilon$ describing the imperfections. When $\epsilon$ is nonzero, the truncated function of $f = 4p(1-p)$ falls into the classical Bernoulli factory and hence can be constructed via $p$-coins. However, the number of classical coins $N$ required to construct $f(p)$ scales poorly with $\epsilon$; see the Supplemental Material [16] for more details. In the experiment, we need to implement high-fidelity state preparation and measurement to reduce $\epsilon$ as small as possible in order to faithfully demonstrate the quantum advantage.

In the following, we focus on the preparation and the measurement of the $p$-quoin, and on how to construct an $f(p) = 4p(1-p)$ coin via necessary classical processing. Here, we emphasize that the quantum circuit for realizing the operations should be independent of $p$. In demonstration, we fix the measurement setting and prepare $p$-quoins for various $p$ values.

*Experimental realization.*—We choose a superconducting qubit system to prepare $p$-quoins. Superconducting quantum systems have made tremendous progress in the last decade, including a realization of long coherence times, showing great stability with fast and precise qubit manipulations, and demonstrating high-fidelity quantum nondemolition (QND) qubit measurement. Thus, it serves as a perfect candidate for our test.

In our experiment, we employ the so-called circuit quantum electrodynamics architecture [20]. A superconducting transmon qubit (our quoin) is located in a waveguide trench and dispersively couples to two 3D cavities [21–23] as shown in Fig. 2. The transmon qubit has a transition frequency of $\omega_q/2\pi = 5.577$ GHz, an anharmonicity $\alpha_q/2\pi = -246$ MHz, an energy relaxation time $T_1 = 9$ $\mu$s, and a Ramsey time $T_2^* = 7$ $\mu$s. The larger cavity has a resonant frequency of $\omega_c/2\pi = 7.292$ GHz and a decay rate of $\kappa/2\pi = 3.62$ MHz, which provides a fast way of reading out the qubit state through their strong dispersive interaction with a dispersive shift $\chi/2\pi = -4.71$ MHz. As we focus on exhibiting a quantum advantage solely with a single quantum system, the smaller cavity with a higher resonant frequency is not used and remains in a vacuum state. This higher frequency cavity can potentially be used as another $p$-quoin in future experiments [24]. In this case, joint measurement can be performed on two $p$-quoins, which may save the resource. For now, we focus on single-qubit operations.

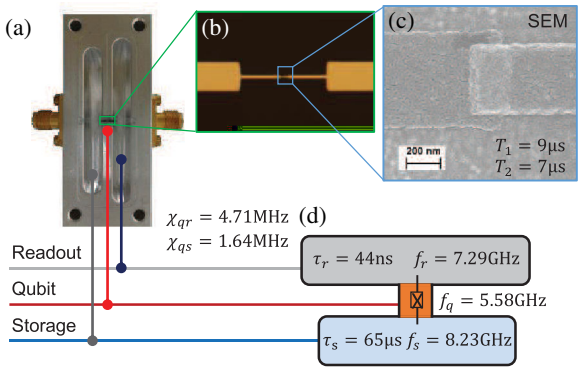


FIG. 2. Experimental setup. (a) Optical image of a transmon qubit located in a trench, which dispersively couples to two 3D Al cavities. (b) Optical image of the single-junction transmon qubit. (c) Scanning electron microscope image of the Josephson junction. (d) Schematic of the device with the main parameters. In our experiment, the higher frequency cavity is not used and always remains in vacuum, which can be used as another $p$-quoin in future experiments [24]. Note that the highlighted boxes in (a) and (b) are not to scale and are intended for illustrative purposes only.

The output of the readout cavity is connected to a Josephson parametric amplifier (JPA) [25,26], operating in a double-pumped mode [27,28] as the first stage of amplification between the readout cavity, at a base temperature of 10 mK, and the high electron mobility transistor, at 4 K. To minimize pump leakage into the readout cavity and achieve a longer $T_2^*$ dephasing time, we operate the JPA in a pulsed mode. The readout pulse width has been optimized to 180 ns with a few photons in order to have a high signal-to-noise ratio. This JPA allows for a high-fidelity single-shot readout of the qubit state. The overall readout fidelity of the qubit measured for the ground state $|0\rangle$ when initially prepared at $|0\rangle$ by a postselection is 0.996, demonstrating the high QND nature of the readout, while the fidelity for the excited state $|1\rangle$ is slightly lower, 0.943 (see the Supplemental Material [16]). The loss of both fidelities is predominantly limited due to the $T_1$ process during both the waiting time of the initialization measurement (300 ns) and the qubit readout time (180 ns).

Because of stray infrared photons and other background noise, our qubit has an excited state population of about 8.5% in the steady state. The high QND qubit measurement allows us to eliminate these imperfections by performing an initialization measurement to purify the qubit by only selecting the ground state for the following experiments [29]. The measurement pulse sequences for preparing quoins can be found in the Supplemental Material [16]. It is worth mentioning that our superconducting system always yields a detection result once the measurement is performed, which is very challenging for other implementations, such as lossy photonic systems.

We apply an on-resonant microwave pulse to rotate the qubit to an arbitrary angle $\theta$ along the $Y$ axis, $R_\theta^Y = \exp(-i\sigma_y\theta/2)$, where $\sigma_y$ is the Pauli matrix, for a preparation of any $p = \cos^2(\theta/2)$-quoins. We choose a Gaussian envelope pulse truncated to $4\sigma = 24$ ns for the rotation operations. We also use the so-called derivative removal by adiabatic gate [30] technique to minimize qubit leakage to higher levels outside the computational space. A randomized benchmark calibration [31–34] shows that the $R_{\pi/2}^Y$ gate fidelity itself is about 0.998, mainly limited by the

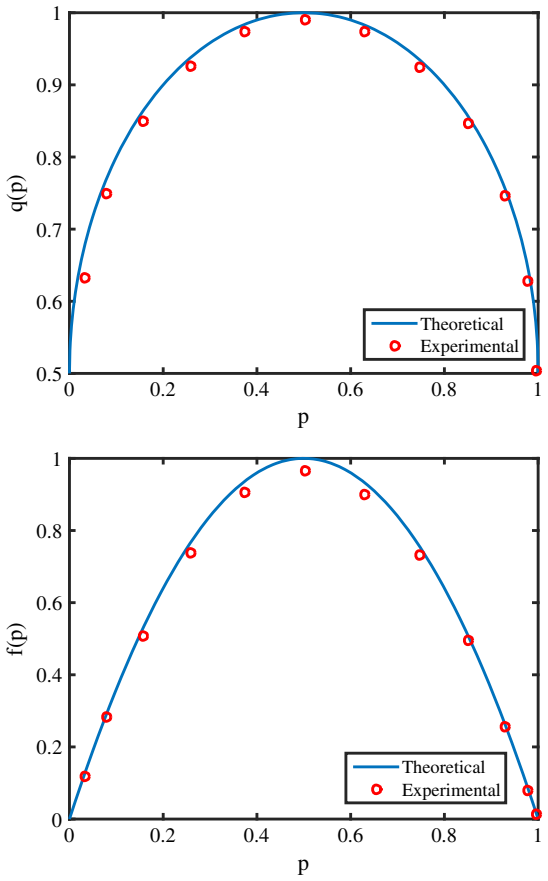


FIG. 3. Theoretical and experimental results for the (a) $q$-coin and (b) $f(p) = 4p(1-p)$-coin. Here, the number of experiment data for the $p$-quoins is on the order of $10^7$ and the number for the $f(p)$-coin is on the order of $10^6$. On average, we need about 20 $p$-quoins to construct an $f(p)$-coin. The standard deviations of $p, q$, and $f(p)$ are of the order of $10^{-4}$; thus, they are not plotted in the figure.

qubit decoherence (see the Supplemental Material [16]). The final measurement for the quoins is along either the $Z$ axis or the $X$ axis. The measurement along the $X$ axis is realized by applying an extra $R^{-Y}_{\pi/2}$ rotation (Hadamard transformation), followed by a $Z$-basis measurement.

In our experiment, the $q$-coins as defined in Eq. (4) are implemented, which are also classically impossible [35] when regarded as a function of $q$. We plot the experiment result of the $q$-coins in Fig. 3(a) and the result of the $f(p) = 4p(1-p)$-coins by following the protocol in Table I in Fig. 3(b). The experimentally realized values of $q_{\mathrm{exp}}$ and $f_{\mathrm{exp}}(p)$ are sampled from the observed coins, which match well with the theoretical predictions. By implementing state preparation, operation, and measurement with high fidelities, we are able to achieve $q_{\mathrm{exp}}(1/2) = 0.990$ and $f_{\mathrm{exp}}(1/2) = 0.965$, which can be well modeled by the truncated function defined in Eq. (6) with $\epsilon = 0.010$ and $\epsilon = 0.035$, respectively.

*Discussion.*—The classical Bernoulli factory cannot produce exact $q$- and $f(p) = 4p(1-p)$-coins with a finite number of usages of $p$-coins. In practice, the implemented function may deviate from the desired one due to device imperfections. In this case, the practically realized coins may be constructible with classical means, though the number of classical coins required may increase drastically with decreasing deviation. Focusing on the truncated function defined in Eq. (6), we present a classical protocol for simulating the experiment data $f_{\mathrm{exp}}(p)$ with $\epsilon = 0.035$ in the Supplemental Material [16]. It is shown that, on average, more than $10^4$ classical $p$-coins are required for constructing the truncated function, which is much larger than the average number of quoins (about 20) used in our protocol [36]. For the $q$-coin, as the deviation is smaller, the classical simulation is even harder. In the Supplemental Material [16], we show that more than $10^5$ classical coins are needed for the truncated function, while our quantum protocol only requires one quoin.

From the experimental perspective, the small deviation $f_{\mathrm{exp}}(1/2)$ from unity in the ideal case is dominated by qubit decoherence. With better qubit coherence times of $T_1, T_2 \sim 100\ \mu$s achieved recently [37], we expect the deviation of $f_{\mathrm{exp}}(p)$ from $f_{th}(p)$ to be an order of magnitude lower. In the future, a more accurate quantum Bernoulli factory could be realized and the classical simulation will eventually become intractable.

In a quantum Bernoulli factory, the only resource that is responsible for constructing a classically impossible function is the quantumness of single qubits—coherence. Our experiment also involves only single-qubit operations and hence proves the quantum advantage solely using coherence without multipartite correlations. Recently, a coherence framework [3] was proposed in which coherence could be measured quantitatively. Along these lines, it would be interesting to see whether the advantage of constructing $f(p)$ from $p$-quoins is directly related to the coherence of the $p$-quoins. Note that the Bernoulli factory is a randomness process. From the close relation between randomness and coherence [9], we expect that a general $p$-quoin with a larger coherence would have an advantage over a $p$-quoin with a smaller coherence.

Our experiment verification sheds light on a fundamental question about what is the essential resource for quantum information processing, which may stimulate the search for more protocols that show quantum advantages without multipartite correlations. Considering the conversion from coherence to multipartite correlation [38], investigating the power of coherence may also be helpful in understanding the power of multipartite correlation and universal quantum computation [39].

It is noteworthy that entanglement can be exploited to save resources in the quantum Bernoulli factory, which provides an extra advantage for randomness processing [10]. Extending our implementation to multiqubit systems can serve to verify this extra quantum advantage. When considering practical imperfections, multiple-qubit

operations generally have a lower fidelity of measurement. Striking a balance between the saving of resources and decoherence due to multiple-qubit interactions, it is interesting to see whether multipartite correlation can display an extra advantage in practice. As we are focusing on proving the advantage only with coherence, we leave such an extension and its discussion to future works.

We acknowledge Z. Cao, H. Dale, E. Ginossar, D. Jennings, T. Rudolph, D. Schuster, and H. Zhou for the insightful discussions and thank M. Chand and T. Roy for the help with the parametric amplifier measurements. This work was supported by the National Basic Research Program of China Grants No. 2011CBA00300 and No. 2011CBA00301, the 1000 Youth Fellowship program in China, and by the National Natural Science Foundation of China Grant No. 11474177.

X. Y. and K. L. contributed equally to this Letter.

*luyansun@tsinghua.edu.cn
†xma@tsinghua.edu.cn

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[2] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).
[3] T. Baumgratz, M. Cramer, and M. B. Plenio, Phys. Rev. Lett. **113**, 140401 (2014).
[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE Press, New York, 1984), p. 175.
[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[7] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[8] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96), Philadelphia, 1996* (ACM, New York, 1996), p. 212.
[9] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Phys. Rev. A **92**, 022124 (2015).
[10] H. Dale, D. Jennings, and T. Rudolph, Nat. Commun. **6**, 8203 (2015).
[11] S. Asmussen, P. W. Glynn, and H. Thorisson, ACM Trans. Model. Comput. Simul. **2**, 130 (1992).
[12] K. Latuszynski, I. Kosmidis, O. Papaspiliopoulos, and G. O. Roberts, Random Struct. Algorithms **38**, 441 (2011).
[13] J. Von Neumann, Appl. Math Ser. **12**, 36 (1951).
[14] M. S. Keane and G. L. O'Brien, ACM Trans. Model. Comput. Simul. **4**, 213 (1994).
[15] A complete definition is $f(p) = 2p$ when $p \in [0, 1/2]$ and $f(p) = 2(1-p)$ when $p \in (1/2, 1]$.
[16] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.010502 for a mathematical proof of the protocol, a simulation method to the experiment, and details for the experimental setup and results.
[17] Ş. Nacu, Y. Peres *et al.*, Ann. Appl. Probab. **15**, 93 (2005).
[18] E. Mossel and Y. Peres, Combinatorica **25**, 707 (2005).
[19] A. C. Thomas and J. H. Blanchet, arXiv:1106.2508.
[20] A. Wallraff, D. I. Schuster, A. Blais, L. Frunzio, R.-S. Huang, J. Majer, S. Kumar, S. M. Girvin, and R. J. Schoelkopf, Nature (London) **431**, 162 (2004).
[21] G. Kirchmair, B. Vlastakis, Z. Leghtas, S. E. Nigg, H. Paik, E. Ginossar, M. Mirrahimi, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, Nature (London) **495**, 205 (2013).
[22] B. Vlastakis, G. Kirchmair, Z. Leghtas, S. E. Nigg, L. Frunzio, S. M. Girvin, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, Science **342**, 607 (2013).
[23] L. Sun, A. Petrenko, Z. Leghtas, B. Vlastakis, G. Kirchmair, K. M. Sliwa, A. Narla, M. Hatridge, S. Shankar, J. Blumoff, L. Frunzio, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, Nature (London) **511**, 444 (2014).
[24] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, Phys. Rev. Lett. **111**, 120501 (2013).
[25] M. Hatridge, R. Vijay, D. H. Slichter, J. Clarke, and I. Siddiqi, Phys. Rev. B **83**, 134501 (2011).
[26] T. Roy, S. Kundu, M. Chand, A. M. Vadiraj, A. Ranadive, N. Nehra, M. P. Patankar, J. Aumentado, A. A. Clerk, and R. Vijay, Appl. Phys. Lett. **107**, 262601 (2015).
[27] A. Kamal, A. Marblestone, and M. H. Devoret, Phys. Rev. B **79**, 184301 (2009).
[28] K. W. Murch, S. J. Weber, C. Macklin, and I. Siddiqi, Nature (London) **502**, 211 (2013).
[29] D. Ristè, J. G. van Leeuwen, H.-S. Ku, K. W. Lehnert, and L. DiCarlo, Phys. Rev. Lett. **109**, 050507 (2012).
[30] F. Motzoi, J. M. Gambetta, P. Rebentrost, and F. K. Wilhelm, Phys. Rev. Lett. **103**, 110501 (2009).
[31] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Phys. Rev. A **77**, 012307 (2008).
[32] C. A. Ryan, M. Laforest, and R. Laflamme, New J. Phys. **11**, 013034 (2009).
[33] E. Magesan, J. M. Gambetta, B. R. Johnson, C. A. Ryan, J. M. Chow, S. T. Merkel, M. P. da Silva, G. A. Keefe, M. B. Rothwell, T. A. Ohki, M. B. Ketchen, and M. Steffen, Phys. Rev. Lett. **109**, 080505 (2012).
[34] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. White, J. Mutus, A. Fowler, B. Campbell *et al.*, Nature (London) **508**, 500 (2014).
[35] The function $q(p)$ is defined in Eq. (4). It is straightforward to check to see that $q(1/2) = 1$, indicating that it is classically impossible.
[36] Strictly speaking, the quantum advantage demonstrated here is a weaker version of the one mentioned at the beginning of the Letter, where the function is classically impossible to construct.
[37] C. Rigetti, J. M. Gambetta, S. Poletto, B. L. T. Plourde, J. M. Chow, A. D. Córcoles, J. A. Smolin, S. T. Merkel, J. R. Rozen, G. A. Keefe, M. B. Rothwell, M. B. Ketchen, and M. Steffen, Phys. Rev. B **86**, 100506 (2012).
[38] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Phys. Rev. Lett. **115**, 020403 (2015).
[39] M. Howard, J. Wallman, V. Veitch, and J. Emerson, Nature (London) **510**, 351 (2014).