Fault-tolerant quantum random-number generator certified by Majorana fermions

Dong-Ling Deng[1,2,*] and Lu-Ming Duan[1,2]

[1]*Department of Physics, University of Michigan, Ann Arbor, Michigan 48109, USA*
[2]*Center for Quantum Information, IIIS, Tsinghua University, Beijing, China*

(Received 27 November 2012; published 23 July 2013)

Braiding of Majorana fermions gives accurate topological quantum operations that are intrinsically robust to noise and imperfection, providing a natural method to realize fault-tolerant quantum information processing. Unfortunately, it is known that braiding of Majorana fermions is not sufficient for the implementation of universal quantum computation. Here we show that topological manipulation of Majorana fermions provides the full set of operations required to generate random numbers by way of quantum mechanics and to certify its genuine randomness through violation of a multipartite Bell inequality. The result opens a perspective to apply Majorana fermions for the robust generation of certified random numbers, which has important applications in cryptography and other related areas.

DOI: 10.1103/PhysRevA.88.012323 PACS number(s): 03.67.−a, 03.65.Ud, 05.30.Pr, 71.10.Pm

I. INTRODUCTION

The complex-valued solutions to the Dirac equation predict that every elementary particle should have a complex-conjugate counterpart, namely, an antiparticle. For example, an electron has a positron as its antiparticle. However, in 1937, Majorana [1] showed that the complex Dirac equation can be modified to permit real wave functions, leading to the possible existence of so-called *Majorana fermions*, which are their own antiparticles [2]. In condensed-matter physics, Majorana fermions may appear as elementary quasiparticle excitations. To search for Majorana fermions, several proposals have been made in recent years, including the $\nu = 5/2$ fractional quantum Hall system [3,4], topological insulator (TI)–superconductor (SC) interface [5], interacting quantum spins [6], chiral p-wave superconductors [7], and spin-orbit coupled semiconductor thin films [8] or quantum nanowires [9,10] in the proximity of an external s-wave superconductor. Based on these proposals, experimentalists have made great progress recently. For instance, Ref. [11] reported an experimental observation of the coexistence of the superconducting gap and the topological surface state in the $\mathrm{Bi_2Se_3}$ thin film as a step towards the realization of Majorana fermions. More recently, a signature of Majorana fermions in a hybrid superconductor-semiconductor nanowire device has been reported [12], which has raised strong interest in the community.

Majorana fermions are exotic particles classified as non-Abelian anyons with fractional statistics, and braiding between them gives nontrivial quantum operations that are topological in nature. These topological quantum operations are intrinsically robust to noise and experimental imperfection, so they provide a natural solution to the realization of fault-tolerant quantum gates. The application of Majorana fermions in the implementation of fault-tolerant quantum computation has raised great interest [4,6]. Unfortunately, braiding of Majorana fermions is not sufficient yet for the realization of universal quantum computation [4], and we need assistance from additional nontopological quantum gates which are prone to the influence of noise.

In this paper, we show that the topological manipulation of Majorana fermions alone can be used to realize a quantum random-number generator in a fault-tolerant fashion and to certify its genuine randomness through the violation of the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [13–15]. Random numbers have tremendous applications in science and engineering [16–18]. However, the generation of genuine random numbers is a challenging task [19]. Any classical device does not generate genuine randomness as it allows a deterministic description in principle. Quantum mechanics is intrinsically random, and one can explore this feature to generate random numbers [20–23]. However, in real experiments, the intrinsic randomness of quantum mechanics is always mixed up with an apparent randomness due to noise or imperfect control of the experiment [19]. The latter can be exploited by an adversary opponent and leads to security loopholes in various applications of randomness. Recently, an interesting idea has been put forward to certify genuine randomness generated by a quantum device through a test of the violation of the Bell-CHSH (Clauser-Horn-Shimony-Holt [24]) inequality [19,25], and the idea has been demonstrated in a proof-of-principle experiment using remote entangled ions [19] . This implementation is not yet fault tolerant as the remote entanglement is sensitive to noise and the quantum gates have a limited precision, which can all lead to security loopholes. We show here that all the operations for the generation and certification of genuine randomness can be realized through the topological manipulation of Majorana fermions. This implementation is inherently fault tolerant and automatically closes security loopholes caused by the influence of noise.

II. CERTIFIED RANDOMNESS VIA MABK INEQUALITY

The implementation of certification of a quantum random-number generator with Majorana fermions is complicated. First of all, one cannot use the Bell-CHSH inequality anymore as proposed in Ref. [19], since it is impossible to violate this inequality through the topological manipulation of Majorana fermions alone [26]. In fact, to observe violations of the

[*] dldeng@umich.edu

CHSH inequality, measurements in the non-Clifford bases are required. However, topological operations on Majorana fermions can only give gates in the Clifford group, and thus are not able to achieve the measurements required for the CHSH inequality violation for randomness certification. Consequently, we have to consider certification of randomness based on the extension of the Bell inequalities in the multiqubit case. For simplicity, here we use the MABK inequality for three logical qubits [13–15]. We show that first, this inequality can be used to certify randomness, and second, the inequality can be tested with topological manipulation of Majorana fermions alone. For the MABK inequality, we consider three qubits, each with two measurement settings. We denote the measurement settings for each qubit by the binary variables x, y, z, and the corresponding measurement outcomes by a, b, c, where $x,y,z,a,b,c = 0,1$. The MABK inequality can be rewritten as [13–15]

$$L \equiv \sum_{(x,y,z)\in\mathcal{S}} \tau(x,y,z)[P(\text{even}|xyz) - P(\text{odd}|xyz)] \leqslant 2, \tag{1}$$

where $\mathcal{S} = \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$ and $\tau(x,y,z)$ is a sign function defined by $\tau(x,y,z) = (-1)^{(x+y+z)/2}$; $P(\text{even}|xyz)$ [$P(\text{even}|xyz)$] is the probability that $a+b+c$ is an even (odd) number when settings (x,y,z) are chosen. The inequality (1) is satisfied by all local hidden variable models. However, in quantum mechanics certain measurements performed on entangled states can violate this inequality. Experimentally, we can repeat the experiment k times in succession to estimate the violation. For each trial, the measurement choices (x,y,z) are generated by an independent identical probability distribution $P(xyz)$. Denote the input string as $\mathcal{I} = (x_1,y_1,z_1;\ldots;x_k,y_k,z_k)$ and the corresponding output string as $\mathcal{O} = (a_1,b_1,c_1;\ldots;a_k,b_k,c_k)$. The estimated violation of the MABK inequality can be obtained from the observed data as

$$\hat{L} = \frac{1}{k} \sum_{(x,y,z)\in\mathcal{S}} \frac{\tau(x,y,z)}{P(xyz)}[N(\text{even}|xyz) - N(\text{odd}|xyz)], \tag{2}$$

where $N(\text{even}|xyz)$ [$N(\text{odd}|xyz)$] denotes the number of trials that we get an even (odd) outcome $a+b+c$ after k times of measurements with the measurement setting (x,y,z).

We need to show that the output string $\mathcal{O}$ from the measurement outcomes contains genuine randomness by proving that it has a nonzero entropy. Let $\{\mathcal{L}_m : 0 \leqslant m \leqslant m_{\max}\}$ be a series of violation thresholds with $\mathcal{L}_0 = 2$ and $\mathcal{L}_{m_{\max}} = 4$, corresponding respectively to the classical and quantum bound. Denote by $\mathcal{D}(m)$ the probability that the observed violation $\hat{L}$ lies in the interval $[\mathcal{L}_m,\mathcal{L}_{m+1})$. We can use the minimum entropy (min-entropy) to quantify the randomness of the output string $\mathcal{O}$ [19,27,28]:

$$E_\infty(\mathcal{O}|\mathcal{I},\mathcal{E},m)_{\mathcal{D}} \equiv -\log_2 \sum_{\mathcal{I},\mathcal{E}} \Big[\max_{\mathcal{O}} \mathcal{D}(\mathcal{O},\mathcal{I},\mathcal{E}|m)\Big], \tag{3}$$

where $\mathcal{E}$ represents the knowledge that a possible adversary has on the state of the device and the maximum is taken over all possible values of the output string $\mathcal{O}$. The probability distribution $\mathcal{D}(\mathcal{O},\mathcal{I},\mathcal{E}|m)$ is defined in Appendix A. Based on a similar procedure as in Ref. [19], we can prove that if $\mathcal{D}(m) > \delta$, the min-entropy of the output string is conditional on the input string and the adversary's information has a lower bound (see the derivation in Appendix A), given by

$$E_\infty(\mathcal{O}|\mathcal{I},\mathcal{E},m)_{\mathcal{D}} \geqslant kf(\mathcal{L}_m - \epsilon) - \log_2(1/\delta), \tag{4}$$

where the parameter $\epsilon \equiv \sqrt{-2(1+4r)^2(\ln \epsilon'^2)}$ with $r = \min P(xyz)$, the smallest probability of the input pairs, and ϵ' is a given parameter that characterizes the closeness between the target distribution $\mathcal{D}(\mathcal{O},\mathcal{I},\mathcal{E})$ and the real distribution after k successive measurements (see Appendix A for an explicit definition). The function $f(\hat{L})$ can be obtained through numerical calculation based on semidefinite programming (SDP) [29] and is shown in Fig. 1. The minimum-entropy bound $kf(\mathcal{L}_m - \epsilon) - \log_2 \frac{1}{\delta}$ and the net entropy versus the number of trials k are plotted in insets (a) and (b) of Fig. 1. Any observed quantum violation with $\hat{L} > 2$ leads to a positive lower bound of the min-entropy, and a positive min-entropy guarantees that genuine random numbers can be extracted from the string $\mathcal{O}$ of the measurement outcomes through the standard protocol of random-number extractors [30]. As some amount of randomness needs to be consumed to prepare the input string according to the probability distribution $P(xyz)$, the scheme here actually realizes a randomness expansion

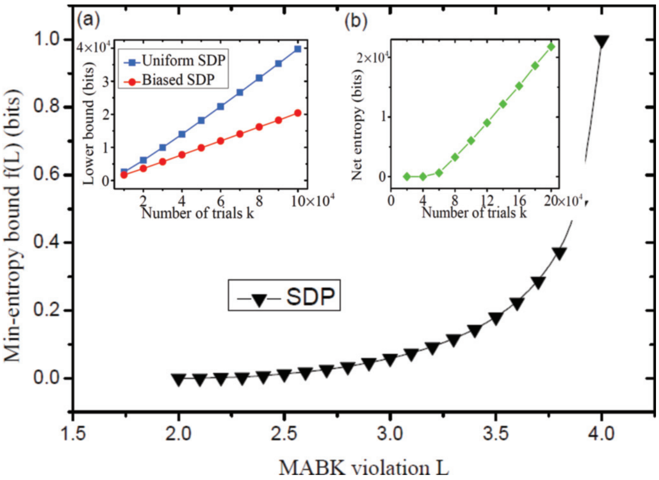

FIG. 1. (Color online) Plot of the function $f(\hat{L})$ vs violation $\hat{L}$ of the MABK inequality. The function is calculated through optimization based on the semidefinite programming, with the details shown in Appendix A. Inset (a) shows the lower bound of the min-entropy $kf(\mathcal{L}_m - \epsilon) - \log_2 \frac{1}{\delta}$ vs the number of trials k. Here we assume an observed MABK violation lies within the interval $3.9 = \mathcal{L}_m \leqslant \hat{L} < \mathcal{L}_{\max} = 4$ with probability δ. The parameters are chosen as $\delta = 0.001$ and $\epsilon' = 0.01$. The bound $kf(\mathcal{L}_m - \epsilon)$ depends on the input probability distribution $P(xyz)$ through the parameter $r = \min_{xyz} P(xyz)$. The blue square line represents the bound under a uniform distribution [$P(xyz) = 1/4$ for all $(x,y,z) \in \mathcal{S}$], while the red dotted line shows the bound under a biased probability distribution with $P(011) = P(101) = P(110) = \alpha k^{-1/2}$ and $P(000) = 1 - 3\alpha k^{-1/2}$ with $\alpha = 10$. It consumes less randomness to generate a biased distribution for the input bits, so the net amount of randomness, defined as the number of output random bits minus that of the input, becomes positive when k is large (typically k needs to be of the order 10^5). Inset (b) plots the net amount of randomness generated after k trails under a biased distribution of the inputs. The parameters are the same as those in inset (a).

device [19,25]. Similar to Ref. [19], we can show that under a biased distribution $P(xyz)$ as shown in Fig. 1 we generate a much longer random output string of length $O(k)$ from a relatively small amount of random seeds of length $O(\sqrt{k}\log_2\sqrt{k})$ when k is large.

III. MAJORANA FERMION IMPLEMENTATION

We now show how to generate and certify random numbers using Majorana fermions. The key step is to generate a three-qubit entangled state and find suitable measurements that lead to violation of the MABK inequality. Majorana fermions are non-Abelian anyons, and their braiding gives nontrivial quantum operations. However, this set of operations is very restricted. First, all the gates generated by topological manipulation of Majorana fermions belong to the Clifford group, and it is impossible to use such operations alone to violate the CHSH inequality [26]. We have to consider instead the multiqubit MABK inequality. Second, it is not obvious that one can violate the MABK inequality as well by using only topological operations. There are two ways to encode a qubit using Majorana fermions, using either two quasiparticles (Majorana fermions) or four quasiparticles (see the details in Appendix A). In the two-quasiparticle encoding scheme, although the braiding gates exhaust the entire two-qubit Clifford group, they cannot span the whole Clifford group for more than two qubits [31]. Furthermore, braiding Majorana fermions within each qubit cannot change the topological charge of this qubit which fixes the measurement basis. Thus, no violation of the MABK inequality can be achieved by using the topological operations alone in the two-quasiparticle encoding scheme. In the four-quasiparticle encoding scheme, it is not straightforward either as braidings in this scheme only allow certain single-qubit rotations and no entanglement can be obtained due to the no-entanglement rule proved already for this encoding scheme [32].

Fortunately, we can overcome this difficulty by taking advantage of the nondestructive measurement of the anyon fusion, which can induce qubit entanglement [33]. In a real physical device, the anyon fusion can be read out nondestructively through the anyon interferometry [34]. In the four-quasiparticle encoding scheme, each qubit is encoded by four Majorana fermions, with a total topological charge 0. The qubit basis states are represented by $|0\rangle \equiv |[(\bullet,\bullet)_{\mathbf{I}},(\bullet,\bullet)_{\mathbf{I}}]_{\mathbf{I}}\rangle$ and $|1\rangle \equiv |[(\bullet,\bullet)_{\psi},(\bullet,\bullet)_{\psi}]_{\mathbf{I}}\rangle$. Here, each $\bullet$ represents a Majorana fermion; $\mathbf{I}$ and ψ represent the two possible fusion channels of a pair of Majorana fermions, with $\mathbf{I}$ standing for the vacuum state and ψ denoting a normal fermion. As explained in Appendix B, a topologically protected two-qubit controlled-NOT (CNOT) gate can be implemented using braidings together with nondestructive measurements of the anyon fusion [33]. To certify randomness through the MABK inequality, we need to prepare a three-qubit entangled state. For this purpose, we need in total 14 Majorana fermions, where 12 of them are used to encode three qubits and another ancillary pair is required for implementation of the effective CNOT gates through the measurement of the anyon fusion. Initially, the logical state is $|\Phi\rangle_i = |000\rangle$. We apply first a Hadamard gate on qubit 1, which can be implemented through a series of anyon braidings as shown in Fig. 2(b), and then two effective CNOT gates on the logical qubits 1, 2, and 2, 3. The final state is the standard three-qubit maximally entangled state $|\Psi\rangle_f = (|000\rangle + |111\rangle)/\sqrt{2}$. After $|\Psi\rangle_f$ is generated, the three qubits can be separated and we need only local braiding and fusion of the anyons within each qubit to perform the measurements in the appropriate bases to generate random numbers and certify them through a test of the MABK inequality.

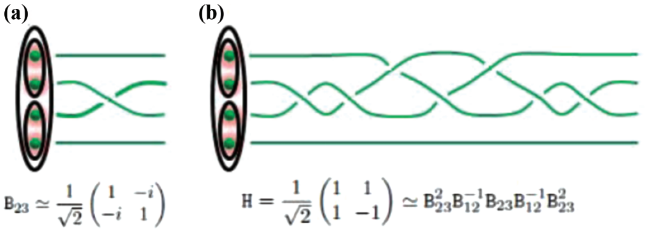
(a)
(b)
$B_{23} \simeq \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$
$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \simeq B_{23}^2 B_{12}^{-1} B_{23} B_{12}^{-1} B_{23}^2$

FIG. 2. (Color online) Illustration of the encoding scheme for a logic qubit using Majorana fermions and two single-qubit operations that can be implemented through anyon braiding. Each qubit is encoded by four Majorana fermions. (a) A counterclockwise braiding of Majorana fermions 2 and 3 implements a unitary gate B_{23} on the corresponding qubit. (b) Implementation of the Hadamard gate through composition of anyon braiding. In both (a) and (b), time flows from left to right and $\simeq$ means equal up to an irrelevant overall phase.

To perform the measurements, we read out each qubit according to the input string $\mathcal{I}$ through nondestructive detection of the anyon fusion. If the input is 0, we first braid the Majorana fermions to implement a Hadamard gate H on this qubit [as shown in Fig. 2(b)], and then measure the fusion of the first two Majorana fermions within each qubit. The measurement outcome is 0 (1) if the fusion result is $\mathbf{I}$ (ψ). If the input is 1, we first braid the Majorana fermions to implement a B_{23} gate [see Fig. 2(a)] on this qubit before the same readout measurement. For instance, with the input $(x,y,z) = (0,1,1)$, we apply a Hadamard gate to the first qubit and B_{23} gates to the second and the third qubits, followed by the nondestructive measurement of fusion of the first two Majorana fermions in each qubit. Under the state $|\Psi\rangle_f$, the conditional probability of the measurement outcomes (a,b,c) under the measurement setting (x,y,z) for these three qubits is give by

$$P(abc|xyz) = |\langle abc|(U_x U_y U_z)|\Psi\rangle_f|^2, \qquad (5)$$

where $U_0 = H$ and $U_1 = B_{23}$. With this conditional probability, we find the expected value of $\hat{L}$ defined in Eqs. (1) and (2) is $\hat{L} = 4$, achieving the maximum quantum violation of the MABK inequality. All the steps for measurements and state preparation are based on the topologically protected operations such as anyon braiding or nondestructive detection of the anyon fusion, so the scheme here is intrinsically fault tolerant and we should get the ideal value of $\hat{L} = 4$ if the Majorana fermions can be manipulated at will in experiments. Such a large violation perfectly certifies genuine randomness of the measurement outcomes.

IV. CONCLUSION

In summary, we have shown that genuine random numbers can be generated and certified through topologically manipulation of Majorana fermions, a kind of anyonic excitation in engineered materials. Such a protocol is intrinsically fault tolerant. Given the rapid experimental progress on the realization of Majorana fermions in real materials [11,12], this protocol offers a promising prospective for the application of these topological particles in an important direction of cryptography with broad implications in science and engineering.

ACKNOWLEDGMENTS

We thank Y. H. Chan, J. X. Gong, and E. Lichko for discussions. This work was supported by the NBRPC (973 Program) 2011CBA00300 (2011CBA00302), the IARPA MUSIQC program, the ARO, and the AFOSR MURI program.

APPENDIX A: CERTIFIED RANDOMNESS CERTIFIED VIA VIOLATIONS OF THE MABK INEQUALITY

In this Appendix, we establish a link between the randomness of the measurement outputs of a quantum system and violation of the MABK inequality. A link between randomness and violation of the Bell-CHSH inequality has been established in Refs. [19,35]. Here, we generalize the result from the two-qubit CHSH inequality to the three-qubit MABK inequality. Consider a quantum nonlocality test on three qubits. Each qubit has two settings of two-outcome measurements, denoted by $\{x,y,z\}$, respectively, for the three qubits. The measurement outputs $\{a,b,c\}$ of this quantum system are characterized by the joint probability distribution $P = \{P(abc|xyz)\}$. Randomness of the outputs $\{a,b,c\}$ is quantified by the min-entropy, defined as $E_\infty(ABC|XYZ) = -\log_2[\max_{abc} P(abc|xyz)]$. With an experimental observation of violation $\hat{L}$ of the MABK inequality, our aim is to find a lower bound on the min-entropy

$$E_\infty(ABC|XYZ) \geqslant f(\hat{L}). \tag{A1}$$

This is equivalent to solving of the following optimization problem [19]:

$$\begin{aligned} P^*(abc|xyz) &= \max P(abc|xyz) \\ &\quad \text{subject to } L = \hat{L}, \\ &\quad P(abc|xyz) = \mathrm{Tr}\big(\rho M_x^a \otimes M_y^b \otimes M_z^c\big), \end{aligned} \tag{A2}$$

where L is defined in Eq. (2) of the main text and $(\rho, M_x^a, M_y^b, M_z^c)$ constitutes a quantum realization of the Bell scenario [36]. Thus, the minimal value of $E_\infty(ABC|XYZ)$ compatible with the MABK violation $\hat{L}$ and quantum theory is given by $E_\infty(ABC|XYZ) = -\log_2[\max_{abc} P^*(abc|xyz)]$. Consequently, to obtain $f(\hat{L})$ we only need to solve (A2) for all possible input and output triplets (x,y,z) and (a,b,c). This can be effectively done by casting it to a *semidefinite program* (SDP) [29]. An infinite hierarchy of conditions that needs to be satisfied by all quantum correlations is introduced in Refs. [37–39]. All these conditions can be transformed to a SDP problem and the hierarchy is complete in the asymptotic limit, i.e., it guarantees the existence of a quantum realization if all the conditions in the hierarchy are satisfied. Generally, conditions higher in the hierarchy are more constraining and thus better reflect the constraints in (A2) and give a tighter lower bound. To obtain a lower bound of the min-entropy for a given MABK violation $\hat{L}$, we use the MATLAB toolbox SeDuMi [40] and solve the SDP corresponding to the certificates between order 1 and order 2 [37]. The result is plotted in Fig. 1 in the main text. From the figure, $f(\hat{L})$ equals zero at the classical point $\hat{L} = 2$ and increases monotonously as the MABK violation $\hat{L}$ increases. For the maximal violation $\hat{L} = 4$, $P^* \approx 0.5003$, corresponding to $f(\hat{L}) \simeq 0.9991$ bits.

Equation (4) in the main text can be derived using arguments similar to those in Refs. [19,28]. The difference is that the Bell scenario in Ref. [19] is based on the two-qubit CHSH inequality, which needs to be extended in our scheme with the three-qubit MABK inequality. Suppose we run the experiments k times and denote the input and output string as $\mathcal{I} = (x_1,y_1,z_1;\ldots;x_k,y_k,z_k)$ and $\mathcal{O} = (a_1,b_1,c_1;\ldots;a_k,b_k,c_k)$, respectively. As in the main text, let $\{\mathcal{L}_m : 0 \leqslant m \leqslant m_{\max}\}$ be a series of MABK violation thresholds, and denote $\mathcal{D}(m)$ the probability that the observed Klyachko-Can-Binicioglu-Shumovsky (KCBS) violation $\hat{L}$ lies in the interval $[\mathcal{L}_m,\mathcal{L}_{m+1})$. Denote by $\mathcal{E}$ the possible classical side information an adversary may have. To derive Eq. (4) in the main text, let us first introduce the following theorem:

Theorem 1. Suppose the experiments are carried out k times and each triplet of inputs (x_i,y_i,z_i) is generated independently with probability $P(xyz)$. Let δ, $\epsilon' > 0$ be two arbitrary parameters and $r = \min\{P(xyz)\}$, then the distribution $P(\mathcal{O}\mathcal{I}\mathcal{E})$ characterizing k successive use of the devices is ϵ' close to a distribution $\mathcal{D}$ such that either $\mathcal{D}(m) \leqslant \delta$ or

$$E_\infty(\mathcal{O}|\mathcal{I},\mathcal{E},m)_{\mathcal{D}} \geqslant kf(\mathcal{L}_m - \epsilon) + \log_2 \delta, \tag{A3}$$

where $\epsilon = (4 + 1/r)\sqrt{-2\ln \epsilon'/k}$.

Equation (A3) is equivalent to Eq. (4) in the main text. Theorem 1 tells us that the distribution P, which characterizes the output $\mathcal{O}$ of the device and its correlation with the input $\mathcal{I}$ and the adversary's classical side information $\mathcal{E}$, is basically indistinguishable from a distribution $\mathcal{D}$ that will be defined below [28]. If we find that the observed MABK violation $\hat{L}$ lies in $[\mathcal{L}_m,\mathcal{L}_{m+1})$ with a non-negligible probability, i.e., $\mathcal{D}(m) > \delta$, the entropy of the outputs $\mathcal{O}$ is guaranteed to have a positive lower bound $kf(\mathcal{L}_m - \epsilon) - \log_2 \frac{1}{\delta}$, that is, the randomness of the outputs is guaranteed to be larger than $kf(\mathcal{L}_m)$ up to epsilonic correction. Theorem 1 can be proved using a similar procedure as in Ref. [28]. Here we omit this proof for conciseness.

It is worthwhile to clarify that in deriving Eq. (A3) we have made the following four assumptions [19,28]: (i) The system can be described by quantum theory; (ii) the inputs at the jth trial (x_j,y_j,z_j) are chosen randomly and their values are revealed to the systems only at step j; (iii) the three qubits are separated and noninteracting during each measurement step; and (iv) the possible adversary has only classical side information. There are no constraints on the states, measurements, or the Hilbert space. Moreover, there is even no requirement that the system behaves identically and independently for each trial. In particular, the system could have an internal memory (classical or quantum) so that the results of the jth trial depend on the previous $j-1$ trials.

We also note that there is a significant difference between the two-qubit scenario in Ref. [19] and our three-qubit scenario here. In the two-qubit case, the randomness can be certified by the no-signaling conditions as well without the assumption of quantum mechanics. However, in our three-qubit scenario, the no-signaling conditions are not sufficient to certify randomness. Actually, we have numerically checked that even for the maximal possible MABK violation $\hat{L}_{\max} = 4$, $P^*(abc|xyz)$ can be equal to the unity for certain (a,b,c) and (x,y,z) if only the no-signaling conditions are imposed, which cannot certify any randomness. A possible reason for this difference is that the MABK inequality only contains four out of eight possible correlations. In other words, the input choice $\mathcal{S}$ is only a subset of $\{(x,y,z)|x,y,z = 0,1\}$. As a result, the no-signaling constraints become less effective.

APPENDIX B: ENCODING AND OPERATION OF QUBITS BY TOPOLOGICAL MANIPULATION OF MAJORANA FERMIONS

In this Appendix, we discuss in detail how to control the logical qubits encoded with Majorana fermions. The fusion rule of Majorana fermions is of the Ising type, $\tau \times \tau \sim \mathbf{I} + \psi$, where τ, $\mathbf{I}$, and ψ stand for a Majorana fermion, the vacuum state, and a normal fermion, respectively. Generally, there are two encoding schemes. The first scheme encodes each logical qubit into a pair of Majorana fermions (two-quasiparticle encoding). When the pair fuse to a vacuum state $\mathbf{I}$, we say that the qubit is in state $|0\rangle$, and when they fuse to ψ, the state is $|1\rangle$. There is also an ancillary pair, which soaks up the extra ψ if necessary to maintain the constraint that the total topological charge must be 0 for the entire system [31,41]. In this encoding scheme, braiding operations of Majorana fermions exhaust the entire two-qubit Clifford group. However, for three or more qubits, not all Clifford gates could be implemented by braiding. The embedding of the two-qubit SWAP gate into a n-qubit system cannot be implemented by braiding [31]. In the two-quasiparticle encoding scheme, no violation of the MABK inequality can be obtained as we cannot change the measurement basis through local braiding of Majorana fermions within each logic qubit.

As we mentioned in the main text, we use the four-quasiparticle encoding scheme where the qubit basis states are represented by $|0\rangle = |[(\bullet,\bullet)_{\mathbf{I}},(\bullet,\bullet)_{\mathbf{I}}]_{\mathbf{I}}\rangle$ and $|1\rangle = |[(\bullet,\bullet)_{\psi},(\bullet,\bullet)_{\psi}]_{\mathbf{I}}\rangle$. Let us first consider braiding operations of Majorana fermions within each logic qubit. Consider four Majorana operators c_i $(i = 1,2,3,4)$ in one logic qubit, which satisfy $c_i^\dagger = c_i$, $c_i^2 = 1$, and the anticommutation relation $\{c_i,c_j\} = 2\delta_{ij}$. The Pauli operators in the computational basis can be expressed as [34]

$$\sigma^x = -ic_2c_3, \quad \sigma^y = -ic_1c_3, \quad \sigma^z = -ic_1c_2. \tag{B1}$$

Unitary operations can be implemented by a counterclockwise exchange of two Majorana fermions $j < j'$:

$$B_{jj'} = e^{(i\pi/4)(ic_jc_{j'})}. \tag{B2}$$

Specifically, we can write down the three basic braiding operators in the computational basis:

$$B_{12} = B_{34} \simeq \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad B_{23} \simeq \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}, \tag{B3}$$

where $\simeq$ means that we ignore an unimportant overall phase. Using these basic braiding operators, a single-qubit Hadamard gate can be implemented as $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \simeq B_{23}^2 B_{12}^{-1} B_{23} B_{12}^{-1} B_{23}^2$. The corresponding braidings are shown in Fig. 2 of the main text. Note that the set of operations implemented through composition of B_{12} and B_{23} are still very limited, however, it is fortunate that B_{23} and H give all the gates that we need for a change of the measurement bases in the test of the MABK inequality. As shown in the main text, we actually get maximum quantum violation of the MABK inequality by randomly choosing either a B_{23} or an H gate on each logic qubit before measurement of the anyon fusion.

With only braiding operations of Majorana fermions, no entangling gate can be achieved for logic qubits in the four-quasiparticle encoding scheme due to the *no-entanglement rule* proved in Ref. [32]. In order to overcome this problem, we need assistance from another kind of topological manipulation: nondestructive measurement of the anyon fusion, which can be implemented through the anyon interferometry as proposed in Ref. [34]. Suppose that we have eight Majorana modes $c_1,c_2,\ldots,c_8$, where the first (last) four modes encode the control (target) qubit, respectively. As shown in Refs. [33,42], a two-qubit controlled phase flip gate $\Lambda(\sigma^z)$ can be implemented through the following identity:

$$\Lambda(\sigma^z) = e^{-(\pi/4)c_3c_4} e^{-(\pi/4)c_5c_6} e^{(i\pi/4)c_4c_3c_5c_6} e^{i\pi/4}. \tag{B4}$$

Note that the first two operations in Eq. (B4) can be directly implemented by braiding operations. The key step is to implement the operation $e^{(i\pi/4)c_4c_3c_5c_6}$. To this end, we use another ancillary pair of Majorana fermions c_9 and c_{10}. We measure fusion of the four Majorana modes $c_4c_3c_6c_9$. The outcome is ± 1, corresponding to either a vacuum state $(+1)$ or a normal fermion (-1). The corresponding projector is given by $\Pi_\pm^{(4)} = \frac{1}{2}(1 \pm c_4c_3c_6c_9)$. Then, we similarly measure fusion of the Majorana modes (operator) $-ic_5c_9$, with the project denoted by $\Pi_\pm^{(2)} = \frac{1}{2}(1 \mp ic_5c_9)$ corresponding to the measurement outcomes ± 1. We have the following relation [33,42]:

$$e^{(i\pi/4)c_4c_3c_5c_6} = 2 \sum_{\eta,\zeta=\pm} U_{\eta\zeta} \Pi_\eta^{(2)} \Pi_\zeta^{(4)}, \tag{B5}$$

where $U_{++} = e^{(\pi/4)c_5c_{10}}$, $U_{+-} = ie^{(\pi/2)c_4c_3} e^{(\pi/2)c_5c_6} e^{(\pi/4)c_5c_{10}}$, $U_{-+} = ie^{(\pi/2)c_4c_3} e^{(\pi/2)c_5c_6} e^{-(\pi/4)c_5c_{10}}$, and $U_{--} = e^{-(\pi/4)c_5c_{10}}$. All the gates $U_{\eta\zeta}$ can be implemented through one or several braiding operations of Majorana fermions. So this identity shows that an effective controlled phase flip gate can be implemented on logic qubits through a combination of anyon braiding and measurement of anyon fusion. Depending on the measurement outcomes (ζ,η) of $c_4c_3c_6c_9$ and $-ic_5c_9$, one can always apply a suitable correction operator $U_{\eta\zeta}$ to obtain the desired operation $e^{(i\pi/4)c_4c_3c_5c_6}$. With controlled phase flip gates, one can easily realize quantum controlled-NOT (CNOT) gate with assistance from the Hadamard operations that can be implemented through the anyon braiding. With CNOT and Hadamard gates, we can then prepare the maximally entangled three-qubit state as required for a test of quantum violation of the MABK inequality.

[1] E. Majorana, Nuovo Cimento **14**, 171 (1937).
[2] F. Wilczek, Nat. Phys. **5**, 614 (2009).
[3] A. Stern, Nature (London) **464**, 187 (2010).
[4] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, Rev. Mod. Phys. **80**, 1083 (2008).
[5] L. Fu and C. L. Kane, Phys. Rev. Lett. **100**, 096407 (2008).
[6] A. Kitaev, Ann. Phys. (N.Y.) **321**, 2 (2006).
[7] N. Read and D. Green, Phys. Rev. B **61**, 10267 (2000).
[8] J. D. Sau, R. M. Lutchyn, S. Tewari, and S. Das Sarma, Phys. Rev. Lett. **104**, 040502 (2010).
[9] R. M. Lutchyn, J. D. Sau, and S. Das Sarma, Phys. Rev. Lett. **105**, 077001 (2010).
[10] Y. Oreg, G. Refael, and F. von Oppen, Phys. Rev. Lett. **105**, 177002 (2010).
[11] M. X. Wang *et al*., Science **336**, 52 (2012).
[12] V. Mourik *et al*., Science **336**, 1003 (2012).
[13] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[14] M. Ardehali, Phys. Rev. A **46**, 5375 (1992).
[15] A. V. Belinskii and D. N. Klyshko, Phys. Usp. **36**, 653 (1993).
[16] J. Ackermann *et al*., Comput. Phys. Commun. **140**, 293 (2001).
[17] P. F. Hultquist, Simulation **57**, 258 (1991).
[18] S. J. Tu and E. Fischbach, Phys. Rev. E **67**, 016113 (2003).
[19] S. Pironio *et al*., Nature (London) **464**, 1021 (2010).
[20] M. Isida and Y. Ikeda, Ann. Inst. Stat. Math. **8**, 119 (1956).
[21] K. Svozil, Phys. Lett. A **143**, 433 (1990).
[22] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[23] T. Jennewein *et al*., Rev. Sci. Instrum. **71**, 1675 (2000).
[24] J. Clauser, F. M. Horne, A. A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[25] R. Colbeck, Ph.D. dissertation, University of Cambridge, 2007.
[26] G. K. Brennen, S. Iblisdir, J. K. Pachos, and J. K. Slingerland, New J. Phys. **11**, 103023 (2009).
[27] R. Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[28] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).
[29] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).
[30] N. Nisan and A. Ta-Shma, J. Comput. Syst. Sci. **58**, 148 (1999).
[31] A. Ahlbrecht, L. S. Georgiev, and R. F. Werner, Phys. Rev. A **79**, 032311 (2009).
[32] S. Bravyi, Phys. Rev. A **73**, 042313 (2006).
[33] S. Bravyi and A. Y. Kitaev, Phys. Rev. A **71**, 022316 (2005).
[34] F. Hassler, A. R. Akhmerov, C. Y. Hou, and C. W. J. Beenakker, New J. Phys. **12**, 125002 (2010).
[35] The theoretical results in Ref. [19] were improperly formulated, and the inaccuracies in formulation were corrected in the recent Refs. [28,43].
[36] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[37] M. Navascues, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).
[38] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).
[39] S. Pironio, M. Navascues, and A. Acin, SIAM J. Optim. **20**, 2157 (2010).
[40] J. Sturm, "SeDuMi, a MATLAB toolbox for optimization over symmetric cones," http://sedumi.mcmaster.ca.
[41] L. S. Georgiev, Phys. Rev. B **74**, 235112 (2006).
[42] S. B. Bravyi and A. Y. Kitaev, Ann. Phys. **298**, 210 (2002).
[43] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A **87**, 012335 (2013).