SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM INFORMATION
APPLIED PHYSICS
COMPUTATIONAL SCIENCE
FLUORESCENCE SPECTROMETRY

Experimental Certification of Random Numbers via Quantum Contextuality

Mark Um[1], Xiang Zhang[1], Junhua Zhang[1], Ye Wang[1], Shen Yangchao[1], D.-L. Deng[1,2], Lu-Ming Duan[1,2] & Kihwan Kim[1]

[1]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, P. R. China, [2]Michigan Center for Theoretical Physics and Department of Physics, University of Michigan, Ann Arbor, MI 48109, USA.

Received
20 December 2012

Accepted
22 March 2013

Published
9 April 2013

Correspondence and requests for materials should be addressed to K.K. (kimkihwan@mail.tsinghua.edu.cn)

The intrinsic unpredictability of measurements in quantum mechanics can be used to produce genuine randomness. Here, we demonstrate a random number generator where the randomness is certified by quantum contextuality in connection with the Kochen-Specker theorem. In particular, we generate random numbers from measurements on a single trapped ion with three internal levels, and certify the generated randomness by showing a bound on the minimum entropy through observation of violation of the Klyachko-Can-Binicioglu-Shumovsky (KCBS) inequality. Concerning the test of the KCBS inequality, we close the detection efficiency loophole for the first time and make it relatively immune to the compatibility loophole. In our experiment, we generate 1×10^5 random numbers that are guaranteed to have 5.2×10^4 bits of minimum entropy with a 99% confidence level.

Random number generation is important for many applications[1,2]. For cryptographic applications, random numbers should have good unpredictability in order to be secure under attack by the adversaries[3]. Genuine random numbers can never be generated by a classical device because any classical device bears in principle a deterministic description. Quantum mechanics, on the other hand, has intrinsic randomness, and thus can be explored to construct a genuine random number generator. There have been many demonstrations of random number generators based on quantum principles[4–14].

Self-certified random number generation is an advance made recently, where the randomness is guaranteed by violation of certain fundamental inequalities[14–16]. In particular, it was proposed in Refs. 14,15 that through violation of the Clauser-Horn-Shimony-Holt (CHSH) inequality, one can certify the generated random numbers in a device-independent fashion that is secure against the adversaries who have only classical side information[17]. The first proof-of-principle experiment for this scheme has been recently demonstrated[14].

We consider here a scenario where the provider of the device is assumed to be honest. However, we still need to physically certify that the random numbers are generated due to the intrinsic uncertainty of quantum mechanics instead of some uncontrolled classical noise process in the device. In this case, we can use quantum contextuality manifested through the violation of certain Kochen-Specker (KS) inequality to certify the generated random numbers[18,19]. Quantum contextuality is a basic property of quantum mechanics, where the measurement outcomes depend on the specific context of the measurements[20,21]. Quantum contextuality would be revealed by violations of some KS inequalities, and such violations can be observed even in a single indivisible system without any entanglement[22–27]. Because there is no need of entanglement, a certification scheme of random numbers based on the KS theorem can significantly simplify the experimental requirement and generate certified random numbers with a much higher speed[18]. A proof-of-principle experimental implementation of this idea has been reported with a photonic system quite recently[18].

A particular type of the KS inequality, the Klyachko-Can-Binicioglu-Shumovsky (KCBS) inequality[22], is convenient for certification of random numbers. Violation of the KCBS inequality has been observed before in a single-photonic system[23]. For experimental test of the KCBS inequality, there are two possible loopholes: the detection efficiency loophole if the detectors only register a subset of data due to their inefficiency, and the compatibility loophole, which occurs if additional assumptions are required to guarantee that the observables with simultaneous assignment of values in the KCBS inequality are compatible with each other and remain identical when their measurement contexts change. The test of the KCBS inequality with the photonic system is immune to the compatibility loophole[23], however, it requires the fair-sampling assumption due to the low photon detection efficiency and thus subject to the detection efficiency loophole.

In this paper, we report a random number generator certified by quantum contextuality with a single trapped ion, which allows us to close the detection efficiency loophole for the first time for the KCBS inequality. For the compatibility, we follow basically the same configurations as in Ref. 23, where errors in compatibible measurement settings only reduce the amount of the violations. Even with experimental noise and imperfections, we get significant violations of the KCBS inequality, which lead to lower bounds the minimum entropy of the generated random string. Compared to the experimental certification based on the CHSH inequality[14], the generation rate of random numbers is increased by about four orders of magnitudes in our experiment, which is important for practical applications.

The paper is organized as follows. First, we introduce the KCBS inequality and show the experimental violation of this inequality. Then, we introduce the relation between the violation of the KCBS inequality and the minimum entropy of the generated random string for the case of an honest provider, and compare the theoretical prediction with our experimental observation. The generated random bits are tested under uniform or biased choice of measurement settings. We conclude the paper by summarizing the results and discussing further improvements of our random number generation scheme.

Results

The KCBS inequality. The Kochen-Specker theorem states that the results of quantum mechanics cannot be fully explained by non-contextual classical theories which assume that the measurement outcomes of a physical system are predetermined and independent of their own and other simultaneous compatible measurements[20,21]. The KCBS inequality illustrates the conflict between quantum mechanics and non-contextual classical theory in the simplest possible system with the Hilbert space dimension $d = 3$[22].

The KCBS inequality is connected with the following simple algebraic equation.

$$a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_1 \geq -3, \qquad (1)$$

where the value of a_i is either 1 or -1. If the values of the observables are predetermined, the average of the left hand of the above equation should be no less than -3, leading to the following inequality:

$$\langle \chi_{KCBS} \rangle = \langle A_1A_2 \rangle + \langle A_2A_3 \rangle + \langle A_3A_4 \rangle + \langle A_4A_5 \rangle + \langle A_5A_1 \rangle \geq -3. \qquad (2)$$

In quantum mechanics, however, the outcomes of A_i do not have predetermined values, which allows violation of the KCBS inequality (2) for a specific state $|\psi_0\rangle$ in systems with $d \geq 3$. In the case of $d = 3$, we denote the bases by $|1\rangle$, $|2\rangle$ and $|3\rangle$ and the observable A_i, represented by $A_i = 1 - 2\,|v_i\rangle\langle v_i|$, is the projector on the axis $|v_i\rangle$. The maximal violation of the KCBS inequality (2) is achieved for the state along the symmetric axis of the pentagram shown in Fig. 1(a). Here $|v_1\rangle = |1\rangle, |v_2\rangle = |2\rangle, |v_3\rangle = R_1(\gamma, 0)\,|v_1\rangle, |v_4\rangle = R_2(\gamma, 0)\,|v_2\rangle, |v_5\rangle = R_1(\gamma, 0)\,|v_3\rangle$ and $|v_1'\rangle = R_2(\gamma,0)|v_4\rangle$, where $\gamma = 51.83^\circ$ and $R_{1,2}$ denote the rotation operations between $|1\rangle$ to $|3\rangle$ and between $|2\rangle$ to $|3\rangle$, respectively. Maximal violation the KCBS inequality is achieved under the state $|\psi_0\rangle = \frac{1}{\sqrt[4]{5}}|1\rangle + \frac{1}{\sqrt[4]{5}}|2\rangle + \sqrt{1-\frac{2}{\sqrt{5}}}|3\rangle$ (2), with the corresponding value $\langle \chi_{KCBS} \rangle = 5 - 4\sqrt{5} \approx -3.944$.

Figure 1(b) shows the scheme for preparation of the initial state $|\psi_0\rangle$ starting from the basis state $|3\rangle$, and Fig. 1(c)–(g) describe the implementation of the measurement configurations along the five axes. To ensure context independence, we emphasize that the measurement configuration of A_i remains the same when it is measured with either A_{i-1} or A_{i+1} (let $A_0 \equiv A_5$, $A_6 \equiv A_1$). For example, the scheme for the measurement A_2 is exactly the same in the first [Fig. 1(c)] and the second stage [Fig. 1(d)]. To move to the second configuration, we perform a rotation between the states $|1\rangle$ and $|3\rangle$, which does not influence the state $|2\rangle$ that corresponds to the observable A_2. Only the observable related to the state $|1\rangle$ is changed from A_1 to A_3.

The configuration for the measurement of A_1 in Fig. 1(c) is not the same as that in Fig. 1(g), which is therefore denoted by A_1'. If A_1 and A_1' are not identical, it is possible to violate the inequality (3) even in classical theory. To solve this problem, similarly to Ref. 23, we use a new inequality that includes the observable A_1' with the form

$$\langle \chi'_{KCBS} \rangle = \langle A_1A_2 \rangle + \langle A_2A_3 \rangle + \langle A_3A_4 \rangle + \langle A_4A_5 \rangle + \left\langle A_5A_1' \right\rangle + \left[1 - \left\langle A_1A_1' \right\rangle\right] \geq -3. \qquad (3)$$

Note that the inequality (3) becomes the original KCBS inequality (2) when $A_1 = A_1'$. Therefore, the difference between two measurements

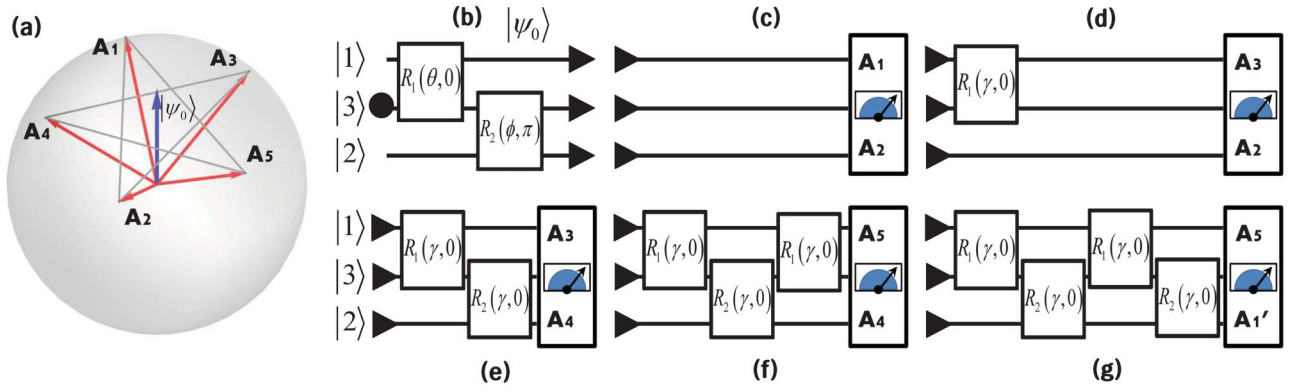

Figure 1 | The representation in 3*d* space and pulse sequences of a state and measurement configurations for the maximal violation of the KCBS inequality (2). (a) The five vectors form a regular pentagram, which represent observables $A_1, A_2, \cdots, A_5$ that are the projectors on them. The vectors related to observables A_i, A_{i+1} are orthogonal, which makes the neighboring observables compatible. The initial state $|\psi_0\rangle$ for the maximal violation is located at the center axis (blue arrow) of the pentagram. The initial state and measurements of the compatible observables are realized by the pulse sequences shown in (b) and (c)-(g). (b) The pulse sequence to prepare $|\psi_0\rangle = \frac{1}{\sqrt[4]{5}}|1\rangle + \frac{1}{\sqrt[4]{5}}|2\rangle + \sqrt{1-\frac{2}{\sqrt{5}}}|3\rangle$. Here, R_1 and R_2 represent the coherent rotations between $|1\rangle$ to $|3\rangle$ and between $|2\rangle$ to $|3\rangle$, respectively, where $\theta = 41.97^\circ$ and $\phi = 64.09^\circ$. The sequence starts from $|3\rangle$ state (black filled circle) after optical pumping. (c)–(g) The pulse sequences for the measurement configurations (c) A_1A_2, (d) A_2A_3, (e) A_3A_4, (f) A_4A_5, (g) A_5A_1', where $\gamma = 51.84^\circ$. The important aspect of the configuration is that the measurement scheme for A_i is perfectly unchanged when it is measured with either A_{i-1} or A_{i+1} except A_1, similarly to the photon realization[23]. The pulse sequence for the confirmation of the identicalness between A_1 and A_1' is shown in Fig. 2(d). For the random number generation, we choose one of the five configurations shown in (c)–(g) based on software random numbers.

decrease the violation that can be obtained in the experiments[23]. Another possible way out is to introduce an empirical parameter to upper bounds the violation of compatibility, which would be similar in spirit to a recent work where a parameter in introduced to bound violation of the locality loophole for test of the Bell inequality[28]. Any imperfection in the initial state preparation or final measurements only leads to a reduction of violation of the KCBS inequality, so a significant violation of this inequality guarantees that the randomness comes from the quantum origin instead of a classical noise process.

Experimental violation of the KCBS inequality. The violation of the KCBS inequality have been observed with single photons[18,23], however, those experiments are subject to the detection efficiency loophole. Here, we present the experimental violation of the KCBS inequality in a single trapped ion. Because of the high detection efficiency for the trapped ion, we close the detection efficiency loophole for the first time for this inequality.

We perform the test of the KCBS inequalities (2) with a single trapped $^{171}Yb^{+}$ ion in a four-rod radio-frequency trap[26,29]. The qubit states are represented by the two internal levels in the $S_{1/2}$ ground-state manifold, with $|F=1, m_F=0\rangle \equiv |\uparrow\rangle$ and $|F=0, m_F=0\rangle \equiv |\downarrow\rangle$. The transition frequency between $|\uparrow\rangle$ to $|\downarrow\rangle$ is $\omega_{HF} = (2\pi)$ 12642.821 MHz, determined by the hyperfine interaction.

The procedure of the experiment consists of Doppler cooling, initialization, coherent operation, and detection (see the Method Section). The initial state preparation and the measurement configurations are shown in Fig. 1(b)-(g), and they are realized by two microwaves with the frequencies ω_1 and ω_2, which produce Rabi oscillations $R_1(\theta_1, \phi_1)$ and $R_2(\theta_2, \phi_2)$ between $|1\rangle$ to $|2\rangle$ and between $|1\rangle$ to $|3\rangle$, respectively. Here, $\theta_{1,2}$ and $\phi_{1,2}$ are controlled by the duration and phase of the microwaves. $R_1(\theta_1, \phi_1)$ and $R_2(\theta_2, \phi_2)$ are have the following explicit forms

$$R_1(\theta_1,\phi_1)=\begin{pmatrix} \cos\frac{\theta_1}{2} & 0 & -ie^{i(\phi_1+\frac{\pi}{2})}\sin\frac{\theta_1}{2} \\ 0 & 1 & 0 \\ -ie^{-i(\phi_1+\frac{\pi}{2})}\sin\frac{\theta_1}{2} & 0 & \cos\frac{\theta_1}{2} \end{pmatrix},$$

$$R_2(\theta_2,\phi_2)=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\frac{\theta_2}{2} & -ie^{-i(\phi_2+\frac{\pi}{2})}\sin\frac{\theta_2}{2} \\ 0 & -ie^{-i(\phi_2+\frac{\pi}{2})}\sin\frac{\theta_2}{2} & \cos\frac{\theta_2}{2} \end{pmatrix}.$$

For experimental convenience, we transform the observable A_i to $V_i = (1 - A_i)/2$, which is assigned to value $v_i = 0$ when photons are detected or $v_i = 1$ when no photons are detected. With V_i, the KCBS inequality (3) is rewritten as

$$\langle \chi'_{KCBS}\rangle = 5 - 4\sum_{i=1}^{5}\langle V_i\rangle + 4\left(\sum_{i=1}^{4}\langle V_i V_{i+1}\rangle + \left\langle V_5 V_1^{'}\right\rangle\right) + \left[4\langle V_1\rangle - 4\left\langle V_1 V_1^{'}\right\rangle\right] \geq -3. \quad (4)$$

We obtain $\langle V_i\rangle$ by mapping the axis v_i to the state $|3\rangle$ and then measuring the probability $P_{|3\rangle}(v_i = 1) = \langle V_i\rangle$ (Fig. 2(b)). For simplicity, let $P_{|3\rangle} = P$. The correlation terms $\langle V_i V_{i+1}\rangle$ are obtained by sequential measurements depicted in Fig. 2(c). First, we transfer V_i on the state $|3\rangle$ and apply the standard fluorescence detection scheme. If we detect photons, the state should not be $|3\rangle$ and we assign $v_i = 0$ to the observable V_i, where the outcome of the correlation term V_iV_j vanishes and no further measurements are needed. If we detect no photons, we assign $v_i = 1$ to the V_i. Then, we apply the swapping microwave π-pulse that converts V_j to $|3\rangle$ before another round of fluorescence detection. If we observe photons, $v_j = 0$, and if no photons, $v_j = 1$. We asign the value 1 to the correlation term V_iV_j only when we detect no photons for both rounds of measurements. We obtain the average of the correlation term $\langle V_iV_j\rangle = P(v_i = v_{i+1} = 1)$ by repeating the same experimental sequence many times[26].

The expectation value $\left\langle V_1 V_1^{'}\right\rangle$ is obtained by the scheme shown in Fig. 2(d). If $V_1 = V_1^{'}$ ideally, the correlation $\left\langle V_1 V_1^{'}\right\rangle$ shoud be same to $\langle V_1\rangle$ since V_1 is projection operator $V_1^2 = V_1$. The state $|1\rangle$ at the beginning of Fig. 1(g) corresponds to the observable V_1, which is exactly the same configuration as in Fig. 1(c). Therefore, if photons are detected ($v_1 = 0$) or not detected ($v_1 = 1$) at the place where V_1 would be measured, photons should be observed ($v_1^{'} = 0$) or not be observed ($v_1^{'} = 1$) for the $v_1^{'}$ shown in Fig. 2 (d). After repeating the

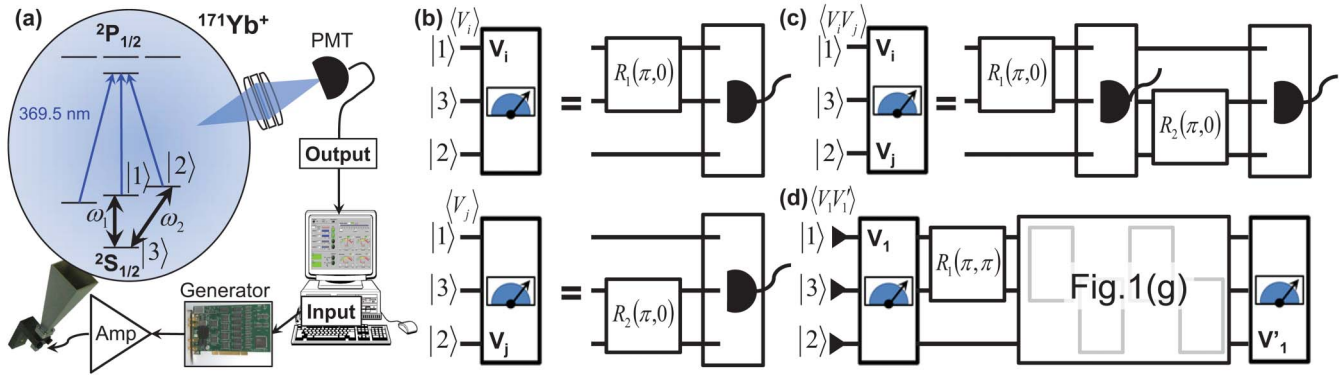

Figure 2 | The trapped $^{171}Yb^{+}$ ion system and detection schemes (a) The schematic diagram of trapped ion $^{171}Yb^{+}$ experimental setup for observing the violation of the KCBS inequality and for generating random numbers certified by the inequality. The three states $|F=1, m_F=0\rangle$, $|F=1, m_F=1\rangle$, and $|F=0, m_F=0\rangle$ in the $S_{1/2}$ ground state manifold are mapped onto $|1\rangle$, $|2\rangle$, and $|3\rangle$, respectively. One of the five measurement configurations in Fig. 1(c)–(g) is chosen by the software generated random number and the pulse sequence of the chosen setting is transfered to the arbitrary wave form generator and is applied to the ion through the amplifier. Depending on the photon counts on the PMT, we assign values on the observables mapped on the state $|3\rangle$. (b) The detection schemes for obtaining results of single observables V_i, V_j. First, V_i or V_j is mapped to the state $|3\rangle$ and apply the standard fluorescent detection method. If we detect photons (no photons), we assign zero (one) on the observable V_i or V_j. After repeating the same pulse sequence and the detection, we obtain the average value of the observable. (c) The sequential measurement scheme for the correlation V_iV_j. V_iV_j has a value one when both of V_i and V_j have one, where no photons are detected at each stage. (d) The experimental confirmation of the identicalness of V_1 and $V_1^{'}$. Ideally, whenever V_1 has a result one (no photons), $V_1^{'}$ should have the same result (no photons). Any imperfection or changes in the system will cause the mismatch of them, which reduces the violation in the extended KCBS inequality (3).

sequence of Fig. 2(d), we acquire the probability that no photons are measured ($P(v_1 = v_1' = 1)$), which gives $\langle V_1 V_1' \rangle$ by definition.

We randomly choose one of the five configurations (c)–(g) of Fig. 1 based on computer generated random numbers and perform the sequential measurements. We change the order of sequential measurements ($V_i V_{i+1}$ or $V_{i+1} V_i$) with equal probability. We occasionally check the overlap of V_1 and v_1'. We repeat the sequences 1×10^5 times and observe $\langle \chi_{KCBS} \rangle = 3.852(0.030)$, which violates the extended KCBS inequality (3,4) by 31 σ. The detailed results of the measurements are summarized in Table 1. We emphasize that our result of the violation cannot be explained by any non-contextual classical theory which does not exploit the compatibility loophole (the detection loophole is closed in our experiment). In other words, any classical part of the system such as technical noise, imperfections and/or unexpected changes of control parameters can not produce the violation. Therefore, as long as we observe the violation of the inequality, we can ensure that the outcomes of our measurements originate from quantum mechanics.

The relation between violation of the KCBS inequality and the min-entropy. We establish the relation between violation of the KCBS inequality (2, 4) and randomness of the generated string from the experiment, similar to the photonic demonstration[18]. We focus on the scenario with an honest provider of the device[17] rather than the extreme adversary scenario where the device has been produced by a malicious manufacturer. Even though we trust the device provider, we still need to ensure that the randomness of the generated sequence is caused by quantum uncertainty instead of technical noise[17]. For this purpose, we assume: (1) the system can be described by quantum theory; (2) the input at lth trial is chosen from a random process that is independent and uncorrelated from the system and its value is revealed to the system only at step l; (3) the outcomes of the corresponding pairs of measurements at step l are compatible (the measurement of one observable does not influence on the marginal distribution of the results of the other observable); (4) the adversary does not have any capability of controlling the inside of the system. The first and the second assumptions here are identical to those made in the certification scheme of Bell's inequality[14]. The third is the contextuality assumption that replaces the role of locality assumption for the Bell inequality. The fourth is an assumption about the honest provider[17].

Table 1 | Experimental results for each of five settings and five joint probabilities for the KCBS inequality (4). We also perform the same experiments with exchanged order. The total trials of the experiment are 1×10^5. The standard deviations of the final result are 0.005 and 0.001 for the single observables and correlations, repectively as shown in the parenthesis. Our experimental test clearly shows the violation of the extended inequality (3) with 31 σ

	$P_{\|3\rangle}$			Correlations		
Setting	Term	Ideal	Result	Term	Ideal	Result
Fig. 1(c)	$\langle V_1 \rangle$		0.452(5)	$\langle V_1 V_2 \rangle$		0.014(1)
	$\langle V_2 \rangle$		0.446(5)	$\langle V_2 V_1 \rangle$		0.015(1)
Fig. 1(d)	$\langle V_2 \rangle$		0.448(5)	$\langle V_2 V_3 \rangle$		0.016(1)
	$\langle V_3 \rangle$		0.436(5)	$\langle V_3 V_2 \rangle$		0.016(1)
Fig. 1(e)	$\langle V_3 \rangle$	0.447	0.428(5)	$\langle V_3 V_4 \rangle$	0	0.014(1)
	$\langle V_4 \rangle$		0.443(5)	$\langle V_4 V_3 \rangle$		0.016(1)
Fig. 1(f)	$\langle V_4 \rangle$		0.464(5)	$\langle V_4 V_5 \rangle$		0.015(1)
	$\langle V_5 \rangle$		0.439(5)	$\langle V_5 V_4 \rangle$		0.014(1)
Fig. 1(g)	$\langle V_5 \rangle$		0.443(5)	$\langle V_5 V_1' \rangle$		0.017(1)
	$\langle V_1' \rangle$		0.431(5)	$\langle V_1' V_5 \rangle$		0.014(1)
Fig. 2(d)				$\langle V_1 V_1' \rangle$	0.447	0.451(5)

$\langle \chi'_{KCBS} \rangle (= -\hat{L} = -3.944) = -3.852(30)$

We consider five sets of measurement configurations $S = \{A_1A_2, A_2A_3, A_3A_4, A_4A_5, A_5A_1\}$, where A_i is the observable with the output $a_i = \pm 1$ and compatible with A_{i-1} and A_{i+1}. We can rewrite the KCBS inequality (2) as

$$L \equiv \sum_{i=1}^{5} \sum_{a_i, a_j} [P(a_i = a_{i+1} | A_i A_{i+1}) - P(a_i \neq a_{i+1} | A_i A_{i+1})] \leq 3, \qquad (5)$$

where $P(a_i = a_{i+1} | A_i A_{i+1})$ or $P(a_i \neq a_{i+1} | A_i A_{i+1})$ is the probability that the output results are the same or different for a chosen measurement setting $A_i A_{i+1}$. Note that we change the sign of the inequality to make the derviation similar to that in Refs. 14,17,30. In our experiment, since we use the observable V_i (result v_i=0,1) intead of A_i and only distinguish the event of $v_i = v_{i+1} = 1$ from others, the Eq. (5) is modified as

$$L \equiv -5 + 4 \sum_{i=1}^{5} P(v_i = 1 | V_i)) - \left\{ 4 \sum_{i=1}^{5} P(v_i = v_{i+1} = 1 | V_i V_{i+1}) \right\} \leq 3, \qquad (6)$$

where $P(v_i = 1 | V_i)$ is the probability that the output result v_i is 1 at a measurement setting V_i. The result of terms inside $\{\cdots\}$ is ideally zero and non-zero positive value can be occurred by experimental errors or imperfections, which only reduces the amount of violation from the optimal. Therefore, we can conclude that the experimental violations of the inequality (6) arise from solely quantum mechanical origin not any classical mean.

In our relization, we estimate the violation of the inequality (6) by repeating the sequences n times and additional runs n_{cc} of the comparibility check, the measurement setting $V_1 V_1'$. The estimation $\hat{L}$ of Eq. (5), obtained from the experimental data, is written as

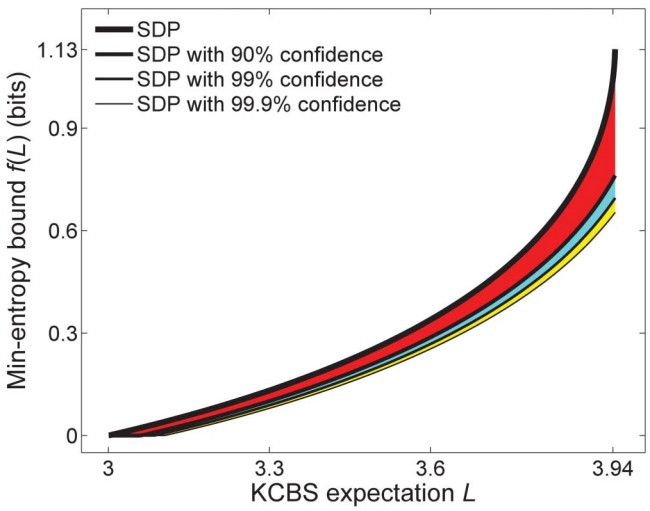

Figure 3 | The min-entropy vs. the violation. The function $f(L)$ in Eq. (8) depending on the violation L of the KCBS inequality (5), which is calculated by semi-definite programming (SDP). The function $f(L-\epsilon)$ at various confidence levels $(1-\epsilon')$ such as 90%, 99% and 99.9% are plotted for the uniform choices of measurement configurations, where $\epsilon \equiv (\mathcal{L}_{m_{max}} + 1/r)\sqrt{-2\ln\epsilon'/n}$ and $r = \min_i P(A_i A_{i+1}) = 1/5$. Here we divide interval with the spacing $\mathcal{L}_m - \mathcal{L}_{m-1} = (\mathcal{L}_{m_{max}} - 3)/10 (= 0.0944)$. Given a measured $\hat{L}$ and confidence level, we can estimate the min-entropy of a generated random string as summarized in Eq. (8). Note that we ignore the term $\log_2 \delta$ in Eq. (8) that does not have dependence on the trial n.

$$\hat{L} = -5 + \frac{4}{n}\sum_{i=1}^{5}\frac{N(v_i=1|V_i)}{P(V_i)} - \left\{\frac{4}{n}\sum_{i=1}^{4}\frac{N(v_i=v_{i+1}=1|V_iV_{i+1})}{P(V_iV_{i+1})} + \frac{N(v_5=v_1'=1|V_5V_1')}{nP(V_5V_1')}\right\} - \left[\frac{4N(v_1=1|V_1)}{nP(V_1)} - \frac{4N(v_1=v_1'=1|V_1V_1')}{n_{cc}}\right], \quad (7)$$

where $N(v_i = 1|V_i)$ or $N(v_i = v_{i+1} = 1|V_iV_{i+1})$ is the number of times that the outcome v_i or v_i and v_{i+1} is one under a measurement setting V_i or V_i and V_{i+1}, respectively. $P(V_i)$ or $P(V_iV_{i+1})$ is the probability with which a measurement configuration V_i or V_i and V_{i+1} is chosen. Note that positive result of terms inside $\{\cdots\}$ and $[\cdots]$ originates from the experimental flaws, which only reduces the amount of violation.

The randomness of a single generated bit v_i from a measurement setting V_i can be characterized by the min-entropy $H_\infty(v_i|V_i) = -\log_2[\max_{v_i}P(v_i|V_i)]$, where $P(v_i|V_i)$ is the conditional probability of obtaining v_i when the input setting V_i and the maximum is taken over all possible values of the output string. The theorem 1 of Ref. 17 shows that the min- entropy of the generated string after n trials is bounded by

$$H_\infty(\mathbf{v}|\mathbf{V}, m) \geq nf(\mathcal{L}_m - \epsilon) + \log_2\delta, \quad (8)$$

where $\mathcal{L}_m(m = 0,1,\cdots m_{max})$ is a series of KCBS violation thresholds with $\mathcal{L}_0 = 3$ the classical bound, and $\mathcal{L}_{m_{max}} = 4\sqrt{5} - 5$ the maximum violation, and $\epsilon \equiv (\mathcal{L}_{m_{max}} + 1/r)\sqrt{-2\ln\epsilon'/n}$, with r the smallest probability of input choices $\min_i P(V_i)$. The parameter ϵ' parameter denotes the closeness between the resulting distribution that characterize k successive uses of the device and another extended distribution that is well defined mathematically. The function f is found by semidefinite programming at various expectations L. Fig. 3 presents how the min-entropies are affected by the confidence levels, $1-\epsilon'$ and $1-\delta$. When we set a high confidence level, $1-\epsilon'$, the bound on the min-entropy reduces as expected. Note that the certified min-entropy is only determined by measured value $\hat{L}$ and the choice of ϵ', independent of experimental details.

Random number results. We perform ten thousand trials to generate random bits as described in the previous section: [**Experimental violation of the KCBS inequality**]. At each trial, we choose one of the five measurement configurations shown in Fig. 1 (c)−(g) by computer-generated random numbers, perform the sequence composed of Doppler cooling, state initialization and rotations for the chosen configuration and finally record the existence of fluorescence (see Method section). As explained, we obtain a random bit, *i.e.*, 1 (or 0) with fluorescence (or no fluorescence) for each trial. The sequence takes about 10 ms, mainly limited by the wave-form loading time to the pulse generator. Note that the random

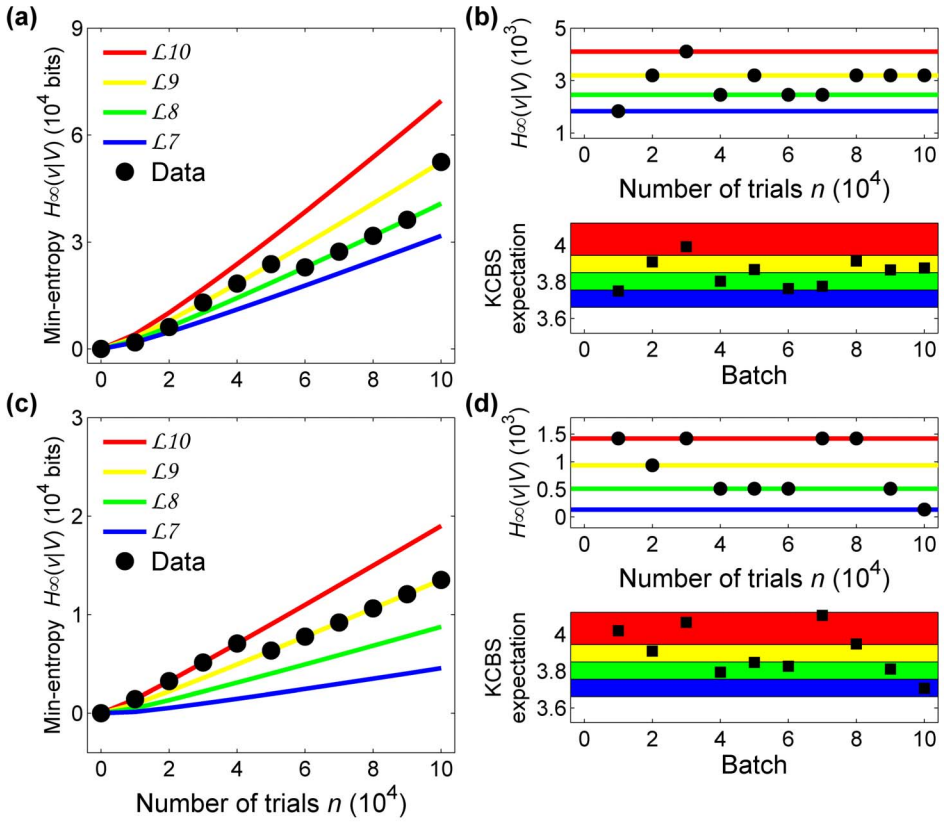

Figure 4 | Comparison between theory and experimental results. (a)(c)The min-entropy $H_\infty(\mathbf{v}|\mathbf{V})$ (8) depending on the number of trials for (a) an uniform distribution of measurement settings $P(V_i) = 1/5$ and (c) a biased distribution with $P(V_1) = 1 - 4q$, $P(V_2) = P(V_3) = P(V_4) = P(V_5) = q$, where $q = 6(100000)^{-1/2}$ with the probablity of errors $\epsilon' = 0.01$ and $\delta = 0.001$. The min-entropies $H_\infty(\mathbf{a}|\mathbf{A})$ (8) are bounded by the relation of the violation $\hat{L}$ of the KCBS inequality (8), where we set the 10 intervals of $\hat{L}$ between $\mathcal{L}_0$ and $\mathcal{L}_{m_{max}}$. The min-entropies are linearly increasing as the number of trial increases and the slopes are basically dependent on the thresholds of the intervals $\mathcal{L}_7 = 3.6610$ (blue), $\mathcal{L}_8 = 3.7554$ (green), $\mathcal{L}_9 = 3.8496$ (yellow), and $\mathcal{L}_{10}(\mathcal{L}_{m_{max}}) = 3.944$ (red). The black dots are obtained from the violation values that were observed at the number of trials. (b)(d) The correlation between the KCBS violations (8) and the min-entropy (8) of the strings for (b) the uniform input choices and (d) the baised settings. Here we divide the total 1×10^5 numbers by 10 division and show the KCBS violations $\hat{L}$ and min-entropies in the division. We can clearly show that the monitor of $\hat{L}$ at each division provides sufficient information to guarantee the min-entropy in the division.

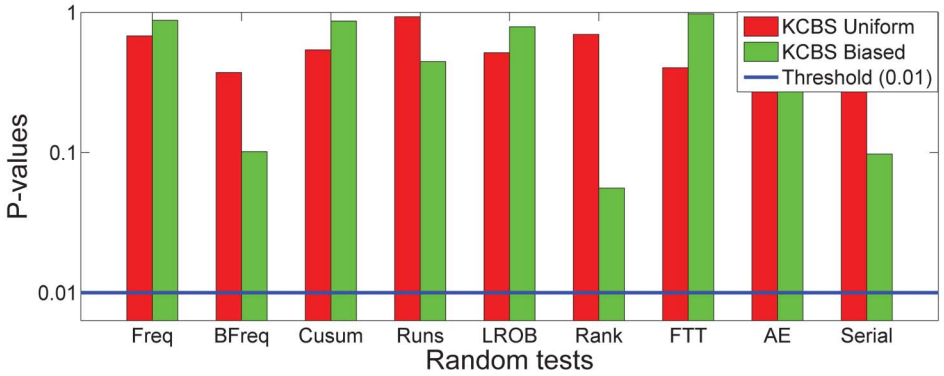

Figure 5 | The results for random tests. The summary for the results of random tests[31] on our generated random numbers. In the tests, we can consider the sequences as random if $P-values$ of the tests are over the threshold that we set, 0.01. All of random numbers pass the listed tests.

generator based on the CHSH inequality produced a random bit per several min.

Figure 4 shows the min-entropies of generated strings discussed in the previous section: [**The relation between violation of the KCBS inequality and the min-entropy**]. We produce a string of length 1×10^5 with uniform choices of the measurement settings, $P(V_i) = 1/5$. As shown in Table 1, we observe the expectation $\hat{L} = 3.852 \pm 0.030$, implying the min-entropy $H_\infty^{uni}(\mathbf{v}|\mathbf{V}) > 5.24 \times 10^4$ with 99% confidence. Note that the other confidence level δ does not have any noticable influence on the bound of min-entropy. Here we used the thresholds of KCBS violations $\mathcal{L}_9 = 3.8496 \left(= \frac{9}{10}(\mathcal{L}_{m_{max}} - 3) \right)$.

Fig. 4 shows clearly the advantage of our certification scheme, *i.e.*, we can guarantee the min-entropy of the generated random string by only monitoring the violation $\hat{L}$ independent of experimental details. Fig. 4(a) shows the accumulated behavior of the min-entropy as the number of experimental trials n increases. The solid lines show the theoretical linear increment of the minentropies and the slopes are determined by only the thresholds $\mathcal{L}_m$. Due to drifts of experimental parameters, the violations $\hat{L}$ are fluctuating from one threshold to another, which accordingly introduces the changes to the min-entropy, accordingly. Fig. 4(b) shows details of the transient behavior of the generated random string. We monitor the violation $\hat{L}$ for each batch of $n = 1 \times 10^4$ trials and estimate the min-entropy in the batch. Fig. 4(b) reveals that the min-entropies are correlated to the violations $\hat{L}$ and completely determined by the thresholds $\mathcal{L}_m$ at given confidence level 99%. Here, we we do not need massive random tests to ensure the amount actual random number in the generated string. The amount of min-entropy of our random numbers is guaranteed by the the measured violations $\hat{L}$, regardless of unexpected changes of experimental parameters.

We also generate random bits with a biased choice of measurement settings, where $P(V_1) = 1 - 4q$, $P(V_2) = P(V_3) = P(V_4) = P(V_5) = q$, and $q = \alpha n^{-1/2}$ with $\alpha = 6$ and $n = 10^5$. We observe basically the same behavior of the min-entropy for the generated stream except for a slightly smaller bound due to the non-uniform setting. We get the min-entropy bound $H_\infty^{bia}(\mathbf{v}|\mathbf{V}) > 1.4 \times 10^4$ from 1×10^5 rounds with violation of $\hat{L} = 3.901$. For the biased choice of measurement settings, the output entropy (1.35×10^4) exceeds the input entropy (1.14×10^4), and we obtain 2.1×10^3 net random bits. For the case of uniform measurement settings, we always need more initial randomness and thus cannot obtain net randomness. This is similar to the random number generation scheme with the CHSH inequality, where to generate net randomness, one always needs to consider nonuniform measurement settings.

Finally, we carry out a series of random tests (see Methods)[31] to examine the quality of our random numbers obtained by collecting the outcomes of the first measurement in each trial. As expected, our generated random numbers passed all the tests. Fig. 5 shows the summary of the test results. Actually the real randomness of our generated strings is already certified by the KCBS inequality, which is a much stronger statement than claiming that the produced numbers pass all the random tests, since no random tests on finite strings should be considered complete.

Discussion

In summary, we have demonstrated violations of the KCBS inequality using a single trapped ion, with the detection efficiency loophole closed for the first time. We use quantum contextuality to certify randomness of the measurement outcomes. The randomness of our device is ensured by observing violations of the inequality independent of experimental details. With our device, we already obtained a net output entropy. The device can generate random numbers with a higher speed, which is important for practical applications.

Methods

Experiment procedure. The experimental procedure consists of Doppler cooling, initialization, coherent operations and detection. After 1 ms Doppler cooling, the internal state of the ion is initialized to $|3\rangle$ by 3 μs standard optical pumping with efficiency 99.1%[26]. The states are coherently manipulated by the microwaves ω_1 and ω_2 that are resonant to the transitions between $|1\rangle$ and $|3\rangle$, and between $|2\rangle$ and $|3\rangle$, respectively. The quantum operations of the microwaves ω_1 and ω_2 are described by the rotation matrix $R_1(\theta_1, \phi_1)$ and $R_2(\theta_2, \phi_2)$, respectively. Here θ_1, θ_2 and ϕ_1, ϕ_2 are controlled by the duration and the phase of the applied microwaves. The 2π times for both Rabi oscillations are adjusted to 29.5 μs, that is $\Omega_{1,2} = (2\pi)$ 33.9 kHz in frequency. The maximum probability of off-resonant excitation $\Omega^2/(\omega_2 - \omega_1)^2$ is about 1.6×10^{-5}, small enough to ensure independence of each Rabi oscillation. The standard fluorescent-detection method enables us to differentiate between one state versus the other two states of a qutrit. We observe on average 10 photons at 369.5 nm for the $|1\rangle$ or the $|2\rangle$ state and detect no photon for the $|3\rangle$ state. The state detection error rates for wrongly registering the state $|3\rangle$ and missing the state $|3\rangle$ are 0.9% and 1.9%, respectively, with the discrimination threshold $n_{\rm ph} = 1$. As shown in Fig. 2(b), we transfer the information of obervable A_i (A_j) by π-pulse and apply the measurement sequence. Then we assign the value $a_i = 1$ ($a_j = 1$) on the obsevable A_i (A_j) when photons detected or $a_i = -1$ ($a_j = -1$) when no photons are detected. After repeating the same experimental procedures, we obtain the $\langle A_i \rangle$ ($\langle A_j \rangle$). Here we emphasize that our setup is not subject to detection loophole and provide a value of the measurement at every trial.

Random test. We apply the random tests that are appropriate for the size of our random numbers, which are 'Frequency', 'Block Frequency', Cumulative Sums (Cusums)', 'Runs', 'Longest-Run-of-Ones in a Block (LROB)', 'Rank', 'Discrete Fourier Transform Test (FTT)', 'Approximate Entropy (AE), 'Serial.' The p-values of all the test, which are the probabilities that an ideal random number generator would produce less random sequence than the tested one. Therefore, a p-value of 0 simply means that the tested sequence appears to be completely non-random, whereas a p-value of 1 implies that the sequence in test appears to be perfectly random. The p-values lie in the open interval (0, 1) and if p-value is larger than a significance level θ, we accept the sequence as random for the test. Typically θ is chosen to be in the range [0.0001, 0.01] and we set $\theta = 0.01$. Note that we use Von-Neumann extractor for the output strings to make uniform distributions, which reduces the size of random numbers to one quarter. We also note that the random tests are different from

guaranteeing the amount of min-entropy in the generated string. In other words, even the data could not pass the random tests but still have the quoted min-entropy.

1. Coddington, P. D. Analysis of random number generators using monte carlo simulation. *Northeast Parallel Architecture Center* Paper 14 (1994).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
3. Goldreich, O. *Foundations of Cryptography* (Cambridge University Press, Cambridge, UK, 2007).
4. Isida, M. & Ikeda, Y. Random number generator. *Ann. Inst. Stat. Math.* **8**, 119–126 (1956).
5. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47**, 595–598 (2000).
6. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
7. Ma, H. Q., Xie, Y. J. & Wu, L. A. A random number generator based on quantum entangled photon pairs. *Chin. Phys. Lett.* **21**, 1961–1964 (2004).
8. Kwon, O., Cho, Y.-W. & Kim, Y.-H. Quantum random number generator using photon-number path entanglement. *Appl. Opt.* **48**, 1774–1778 (2009).
9. Qi, B., Chi, Y.-M., Lo, H.-K. & Qian, L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.* **35**, 312–314 (2010).
10. Gabriel, C. *et al.* A generator for unique quantum random numbers based on vacuum states. *Nature Photonics* **4**, 711–715 (2010).
11. Bustard, P. J. *et al.* Quantum random bit generation using stimulated raman scattering. *Opt. Exp.* **19**, 25173–25180 (2011).
12. Symul, T., Assad, S. M. & Lamb, P. K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* **98**, 231103 (2011).
13. Fiorentino, M., Santori, C., Spillane, S. M. & Beausoleil, R. G. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A* **75**, 032334 (2007).
14. Pironio, S. *et al.* Random numbers certified by bell's theorem. *Nature* **464**, 1021 (2010).
15. Colbeck, R. Quantum and relativistic protocols for secure multi-party computation. *Ph.D. thesis, University of Cambridge* (2007).
16. Vazirani, U. & Vidick, T. Certifiable quantum dice. *Phil. Trans. R. Soc. A* **370**, 3432–3448 (2012).
17. Pironio, S. & Massar, S. Security of practical private randomness generation. *Phys. Rev. A* **87**, 012336 (2013).
18. Deng, D. L. *et al.* Exploring quantum contextuality to generate true random numbers. *arXiv:1301.5364* (2013).
19. Abbott, A. A., Calude, C. S., Conder, J. & Svozil, K. Kochen-specker theorem revisited and strong incomputability of quantum randomness. *arXiv:1207.2029* (2012).
20. Kochen, S. & Specker, E. P. The problem of hidden variables in quantum mechanics. *J. Math. Mech.* **17**, 59–87 (1967).
21. Bell, J. S. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* **38**, 447–452 (1966).
22. Klyachko, A. A., Can, M. A., Binicioğlu, S. & Shumovsky, A. S. Simple test for hidden variables in spin-1 systems. *Phys. Rev. Lett.* **101**, 020403 (2008).
23. Lapkiewicz, R. *et al.* Experimental non-classicality of an indivisible quantum system. *Nature* **474**, 490–493 (2011).
24. Yu, S. & Oh, C. H. State-independent proof of kochen-specker theorem with 13 rays. *Phys. Rev. Lett.* **108**, 020403 (2012).
25. Zu, C. *et al.* State-independent experimental test of quantum contextuality in an indivisible system. *Phys. Rev. Lett.* **109**, 150401 (2012).
26. Zhang, X. *et al.* State-independent experimental tests of quantum contextuality in a three dimensional system. *Phys. Rev. Lett.* **110**, 070401 (2013).
27. Kong, X. *et al.* An experimental test of the non-classicality of quantum mechanics using an unmovable and indivisible system. *arXiv:1210.0961* (2012).
28. Silman, J., Pironio, S. & Massar, S. Device-independent randomness generation in the presence of weak cross-talk. *Phys. Rev. Lett.* **110**, 100504 (2013).
29. Olmschenk, S. *et al.* Manipulation and detection of a trapped Yb^+ hyperfine qubit. *Phys. Rev. A* **76**, 052314 (2007).
30. Fehr, S., Gelles, R. & Schaffner, C. Security and composability of randomness expansion from bell inequalities. *Phys. Rev. A* **87**, 012335 (2013).
31. Rukhin, A. *et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. *NIST special publication* **800–22**, Rev. 1–a (2010).

Acknowledgements

We thank Periklis Papakonstantiou, Dominik Scheder and Xiongfeng Ma for helpful discussion. This work was supported in part by the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, 2011CBA00302, the National Natural Science Foundation of China Grant 61073174, 61033001, 61061130540. KK acknowledges the support from the Thousand Young Talents program.

Author contributions

M.U., X.Z., J.Z. and Y.W. developed the experimental setup for the measurements. M.U., X.Z., J.Z., Y.W. and S.Y. carried out the measurements. M.U. analyzed the data and D.L.D., L.M.D. provided the theoretical support. K.K. supervised the experiment. All authors participated in writing the manuscript.

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Um, M. *et al.* Experimental Certification of Random Numbers via Quantum Contextuality. *Sci. Rep.* **3**, 1627; DOI:10.1038/srep01627 (2013).