SCIENTIFIC REPORTS

OPEN

Corrigendum: Experimental Certification of Random Numbers via Quantum Contextuality

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

Correction to: *Scientific Reports* https://doi.org/10.1038/srep01627, published online 09 April 2013; updated 02 February 2018

The original version of this Article contained an error in the spelling of the author Yangchao Shen, which was incorrectly given as Shen Yangchao.

This error has now been corrected in the PDF and HTML versions of the Article.

In addition, the $\langle V_i V_j \rangle$ terms in Table 1 were omitted from the calculation of $\langle \chi'_{KCBS} \rangle$ in Equation 4. Therefore, in Table 1,

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

should read:

$$\langle \chi'_{KCBS} \rangle (= -\hat{L} = -3.944) = -3.594(34)$$

As a result, in the Abstract,

"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."

should read:

"In our experiment, we generate 1×10^5 random numbers that are guaranteed to have 2.4×10^4 bits of minimum entropy with a 99% confidence level."

In the Results section, under subheading 'Random number results',

"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 $\mathcal{L}_9 = 3.8496$ $(= \frac{9}{10}(\mathcal{L}_{m_{max}} - 3))$."

should read:

"As shown in Table 1, we observe the expectation $\hat{L} = 3.594 \pm 0.034$, implying the min-entropy $H_\infty^{uni}(\mathbf{v}|\mathbf{V}) > 2.44 \times 10^4$ with 99% confidence. Note that the other confidence level δ does not have any noticeable influence on the bound of min-entropy. Here we used the thresholds of KCBS violations $\mathcal{L}_9 = 3.5666$ $(= \frac{6}{10}(\mathcal{L}_{m_{max}} - 3))$."

In the title of Table 1,

"Our experimental test clearly shows the violation of the extended inequality (3) with 31 σ"

should read:

"Our experimental test clearly shows the violation of the extended inequality (3) with 18 σ"

Moreover, the presented data for the biased choice of measurement settings does not show the net randomness after including the terms $\langle V_i V_j \rangle$ in Table 1 for the $\langle \chi'_{KCBS} \rangle$ in Equation 4. it is necessary to double the total experimental round as $n = 2 \times 10^5$ with the new biased distribution parameter $\alpha = 12$ in order to observe the net randomness. Therefore, the contents of the paper related to the biased choice of measurement settings should be corrected as follows.

In the Results section, under subheading 'Random number results',

"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."

should read:

"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 $\alpha = 12$ and $n = 2 \times 10^5$. 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 $H_\infty^{bia}(\mathbf{v}|\mathbf{V}) > 4.0 \times 10^4$ from 2×10^5 rounds with violation of $\hat{L} = 3.692$. For the biased choice of measurement settings, the output entropy (3.95×10^4) exceeds the input entropy (3.28×10^4), and we obtain 6.8×10^3 net random bits."

In the legend of Figure 4,

"(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 $\mathcal{L}_{10} = 3.944$ (red)."

should read:

"(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 $q = 12(200000)^{-1/2}$ with the probability 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."

Figures 4 and 5 based on the corrections of the $\langle \chi'_{KCBS} \rangle$ for the uniform distribution and the new data for the biased choice of measurement setting are shown below as Figures 1 and 2, respectively.

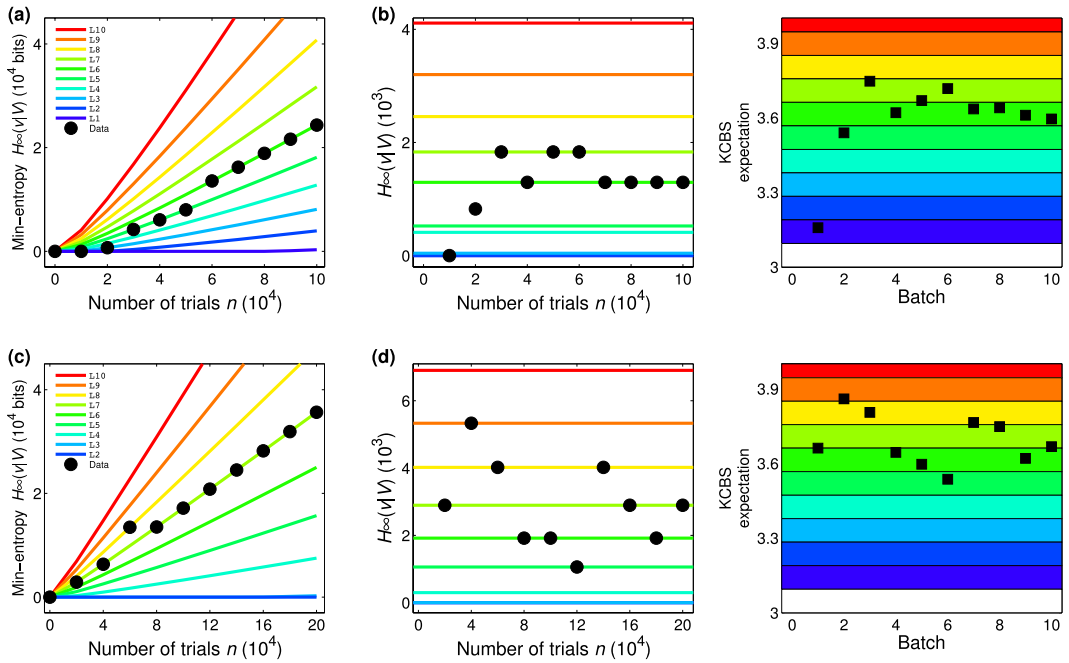

Figure 1.

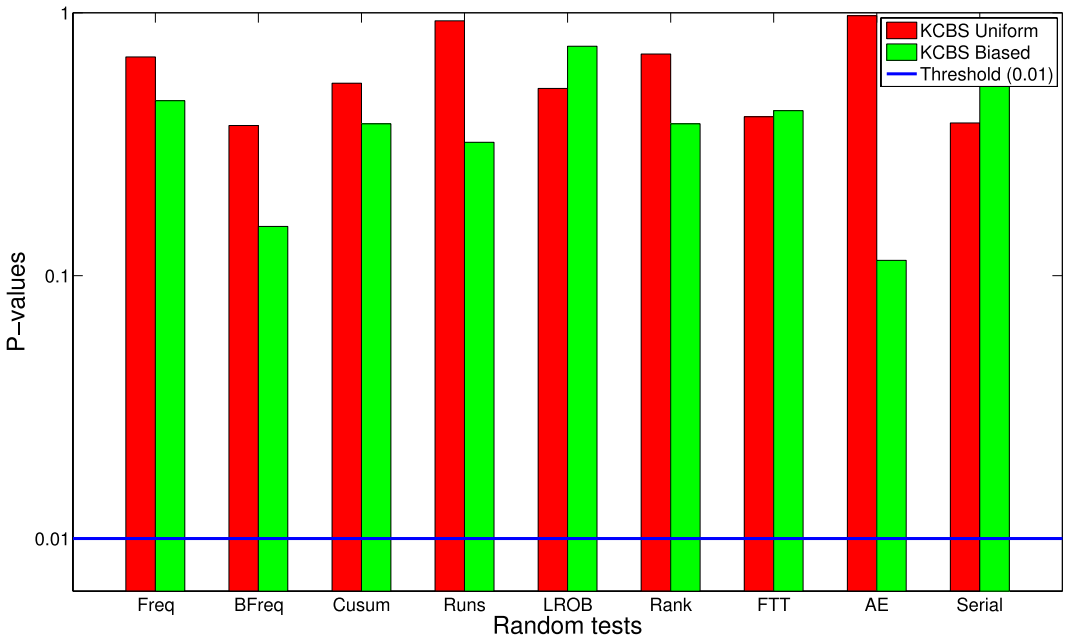

Figure 2.

In addition, this Article contains typographical errors in the Results section, under subheading 'The KCBS inequality'.

"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 $\gamma = 51.83°$ and $R_{1,2}$ denote the rotation operations between $|1\rangle$ to $|3\rangle$ and between $|2\rangle$ to $|3\rangle$, respectively."

should read:

"Here $|v_1\rangle = |1\rangle$, $|v_2\rangle = |2\rangle$, $|v_3\rangle = R_1^{-1}(\gamma, 0)\,|v_1\rangle$, $|v_4\rangle = R_1^{-1}(\gamma, 0)\,R_2(\gamma, 0)\,|v_2\rangle$, $|v_5\rangle = R_1^{-1}(\gamma, 0)\,|v_3\rangle R_2^{-1}(\gamma, 0)\,|v_3\rangle$ and $|v'_1\rangle = R_1(\gamma, 0)^{-1} R_2(\gamma, 0)^{-1} |v_4\rangle$, where $\gamma = 103.68°$ and $R_{1,2}$ denote the rotation operations between $|1\rangle$ to $|3\rangle$ and between $|2\rangle$ to $|3\rangle$, respectively."

In the legend of Figure 1,

"(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 $\theta = 41.97°$ and $\phi = 64.09°$. 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 $\gamma = 51.84°$."

should read:

"(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 $\theta = 83.94°$ and $\phi = 128.18°$. 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 $\gamma = 103.68°$."