New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Higher amounts of loophole-free Bell violation using a heralded entangled source

To cite this article: Shuai Zhao *et al* 2019 *New J. Phys.* **21** 103008

View the article online for updates and enhancements.

You may also like

- Comparing different approaches for generating random numbers device-independently using a photon pair source
V Caprara Vivoli, P Sekatski, J-D Bancal et al.
- Bell violations with entangled and non-entangled optical fields
J Gonzales, P Sánchez, V Avalos et al.
- Randomness in quantum mechanics: philosophy, physics and technology
Manabendra Nath Bera, Antonio Acín, Marek Ku et al.

This content was downloaded from IP address 37.5.240.54 on 13/04/2026 at 13:15

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
10 March 2019

REVISED
13 August 2019

ACCEPTED FOR PUBLICATION
17 September 2019

PUBLISHED
3 October 2019

Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Higher amounts of loophole-free Bell violation using a heralded entangled source

Shuai Zhao[1,2], Wen-Fei Cao[1,2], Yi-Zheng Zhen[1,2], Changchen Chen[3], Li Li[1,2], Nai-Le Liu[1,2], Feihu Xu[1,2] and Kai Chen[1,2]

[1] Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China
[2] CAS Center for Excellence and Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China
[3] Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, United States of America

E-mail: feihuxu@ustc.edu.cn **and** kaichen@ustc.edu.cn

Keywords: quantum key distribution, loophole-free Bell tests, heralded entangled source, device-independent quantum information processing

Supplementary material for this article is available online

Abstract

Loophole-free Bell non-locality test plays a central role in device-independent quantum information processing tasks, such as device-independent quantum random number generation (QRNG) and quantum key distribution (QKD). Inspired by the scheme of heralded spontaneous parametric down conversion (SPDC) source proposed in (Śliwa C and Banaszek K 2003 *Phys. Rev.* A **67** 030101), we present a loophole-free Bell test scheme that employs the heralded type of entangled photon pairs. Our proposal enables a much higher degree of Bell violation with realistic photonic devices over the one using the conventional SPDC source, thus allowing the implementation of device-independent QRNG and QKD with significant advantages. We anticipate that the scheme will enable variously subtle applications in device-independent quantum information processing tasks.

1. Introduction

Bell non-locality [1–4] draws one of the most important distinctions between quantum mechanics and classical mechanics in the sense that Bell nonlocal correlations can not be explained by the local-realistic theory [5]. Despite this fundamental interest, the Bell non-locality has also laid a significant foundation for many promising quantum information processing tasks. Indeed, in a model that reproduces Bell nonlocal correlations, the measurement outcomes cannot be fully determined by sharing local variables. Therefore, once Bell non-locality is certified in a quantum information processing task, the measurement outputs cannot be fully predicted by a third party no matter the mechanism underlying the devices, i.e. *device independent security* [6]. For instance, the Bell non-locality guarantees the security of device-independent quantum key distribution (DI-QKD) [6–11] and device-independent quantum random number generation (DI-QRNG) [12–20]. See [21, 22] for a general discussion on the subjects of QKD and QRNG.

Practically, Bell non-locality is often verified by the violation of a Bell inequality [1]. There have been fruitful results along this route [1–4, 23–27], among which the Clauser–Horne–Shimony–Holt (CHSH) inequality [2] is the simplest in Bell tests. Nevertheless, Bell testing experiments are extremely difficult to conduct due to the potential loopholes [28]. Specifically, we present three well discussed loopholes as follows.

- The *locality* loophole. Once the local parties are not spacelike separated, there could be signals about the measurement sites from one party to influence the measurements at the other party. Specifically, spacelike separations of the event that determines the measurement setting choice at one party and the event that generates the measurement outcome at the other party can close the locality loophole [4].

© 2019 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft

- The *freedom-of-choice* loophole. For the case that the measurement settings are not independent from local hidden variables (LHV), the measurement results would be manipulated arbitrarily. The freedom-of-choice loophole can be closed when the measurement setting choices are generated by true random number generators, and the setting choices events are spacelike separated from the source pairs generation events [29].
- The *fair-sampling* loophole. Supposing the parties select only the detected events and discard the undetected events, fair-sampling assumption states that the subensemble of detected events can represent the total ensemble. However, if the detection efficiency is non-unit, the detection events could be controlled by LHV depending on the measurement settings choices of the parties [30, 31]. The fair-sampling loophole-free (or detection loophole-free) Bell test can be realized by considering all the detected and undetected events, and using sufficiently high efficiency detectors [4].

There have been several experimental Bell tests reported to be loophole-free. For examples, the experiments reported in references [32, 33] are the first two experiments which closed the detection loophole using photons, the experiments in references [34–36] have closed above three loopholes simultaneously, the experiment in [37] has closed the locality loophole and the fair-sampling loophole simultaneously using entangled atoms. It is noteworthy that DI-QRNG has also been realized [18–20]. However, until now the loophole-free Bell tests are still extremely limited even with state-of-the-art technologies. To push forward the application of device-independent quantum information processing, one must overcome a number of practical obstacles such as imperfections of the source of entanglement and the detectors.

As Bell non-locality has been vital for many quantum information processing tasks, it is of great significance for achieving higher amounts of violation of Bell inequalities in Bell tests. Experimentally, the spontaneous parametric down-conversion (SPDC) [38] source has been widely adopted to generate entanglement photon pairs in quantum information processing. However, the maximum loophole-free CHSH value using the conventional entangled SPDC source is only 2.35 even with a unit efficiency detector theoretically [39], which is far from the maximal value of $2\sqrt{2}$ allowed by Tsirelson's bound in quantum theory [40]. The main reason is that vacuum and multi-pair photons dominate the output mode of the conventional SPDC source which will be very harmful to the violation of CHSH inequality.

In this letter, we propose a loophole-free Bell test scheme using entangled photon pairs based on the *heralded* SPDC source proposed in [41]. Owing to its heralding mechanism [41–43], one may expect that higher amounts of violation of Bell inequalities can be achieved using the heralded SPDC source compared with that using the conventional SPDC source. It is demonstrated that the degree of violation for the CHSH inequality using the heralded entangled source can significantly surpass the one using the conventional SPDC source [39] for both non-maximally entangled output modes and maximally entangled output modes. In the ideal case according to our proposal, the maximal violation for CHSH inequality using the heralded entangled source is 2.828, which is approaching the Tsirelson's bound [40]. This result is significantly higher than 2.35 which is the maximal violation for CHSH inequality using multi-mode emission of the conventional SPDC source even with unit detector efficiency [39]. The Clauser–Horne (CH) inequality [3] violation using the heralded entangled source can be two orders of magnitude better than that is reported in [34] for typical experiment parameters. As one of the most promising applications of Bell non-locality, we also present a DI-QKD scheme using the heralded entangled source, and show that one can reduce the lower bound of detector efficiency for positive key rate from 95.3% to 91%, and obtain a 2.62 times higher key generation rate compared with that using the conventional SPDC source.

2. The heralded polarization-entangled source

The heralded entangled source consists of a conventional SPDC source and a linear optical part which is used to herald generations of entangled photon pairs (see appendix C for detail analysis). As shown in figure 1, the coincidence of four detectors D_1, D_2, D_3 and D_4 heralds a successful preparation of one pair of entanglement photons. The output mode of the conventional SPDC source has the form [41, 44]

$$|\Psi\rangle = \sum_{n=0}^{\infty} \lambda_n |\psi_n\rangle, \tag{1}$$

where λ_n is the probability amplitude of the nth order of the output mode, $|\psi_n\rangle$ is the wave function for n pairs of photons. As to the heralded SPDC source, the third order element $|\psi_3\rangle$ is the lowest order that contributes to the coincidence of four detectors [41], and the corresponding output mode is an entangled state

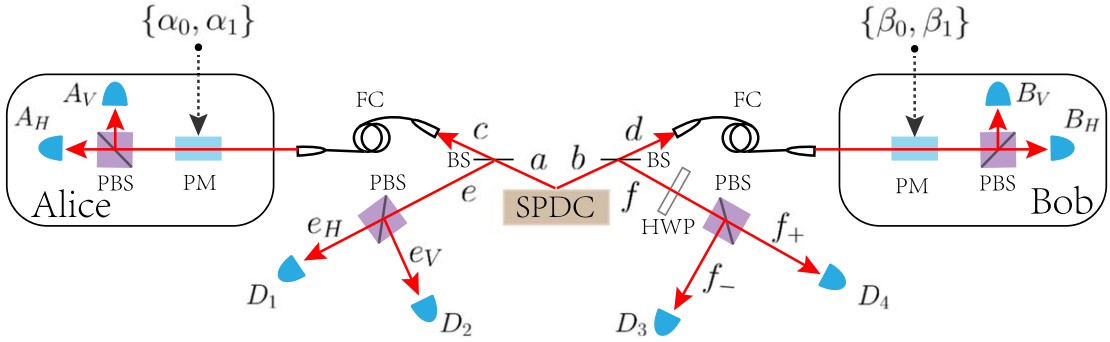

Figure 1. Schematic setup for loophole-free CHSH test using heralded entangled source. *a*, *b*, *c*, *d*, *e* and *f* label the paths of beams, {*H*, *V*} and {+, −} are orthogonal polarization bases. $A_{H(V)}$, $B_{H(V)}$, $D_{1(2)}$ and $D_{3(4)}$ label the corresponding non-photon-number-resolving detectors. $\{\alpha_0, \alpha_1\}$ and $\{\beta_0, \beta_1\}$ label the measurement settings for Alice and Bob. BS: non-polarization beam splitter; HWP: half-wave plate; PM: polarization modulator; PBS: polarization beam splitter; FC: fiber channel; SPDC: spontaneous parametric down-conversion source.

$$|\phi_r\rangle = \frac{1}{\sqrt{r^2+1}}(r|HH\rangle + |VV\rangle), \tag{2}$$

where {*H*, *V*} is an orthogonal polarizing basis, *r* depends on the squeezing parameters associated with the source (see appendix B). When $r = 1$, it reduces to the maximally entangled state

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle). \tag{3}$$

In fact, the components $n \geqslant 4$ will also contribute to the coincidence events of four detectors. The corresponding output modes of the coincidence events for $n \geqslant 4$ will reduce the fidelity of the entanglement pairs. For example, considering the next leading order $|\psi_4\rangle$, after the optimization for the probability of coincidence events caused by the component $|\psi_3\rangle$, the contribution of the next leading order term $|\psi_4\rangle$ to the coincidence events is rather small as analyzed in [41]. In our simulation, we have considered the multiple pair events up to $n = 5$, where the CHSH value contributed by the component of $n \geqslant 6$ is negligible, as compared with that contributed by the dark-count events of $p_d \geqslant 10^{-8}$ [45, 46]. Thus, even though higher orders of output modes of the conventional SPDC source may also contribute to coincidence events, the heralded entangled photon pairs dominate the output state of the heralded entangled source. Based on the advantage of the heralded SPDC source, we explore its potential improvement on Bell tests and quantum information processing tasks.

3. Bell tests using heralded entangled source

3.1. Loophole-free CHSH test using heralded entangled source

The CHSH inequality has been extensively employed in Bell tests. There are two separated players, Alice and Bob, sharing entanglement pairs. Alice randomly chooses a measurement *x* from measurement setting choices $\{\alpha_0 = 0, \alpha_1 = 1\}$ to measure the particle in her side, similarly for Bob with measurement setting choices $y \in \{\beta_0 = 0, \beta_1 = 1\}$. What they obtain are binary results $\{\pm 1\}$, labeled by *i* and *j* for Alice and Bob, respectively. The trial is repeated for many times to accurately estimate the probability distribution $P(ij|xy)$ (see appendix D for details). Alice and Bob then calculate the CHSH value [2]

$$S = \sum_{x,y}(-1)^{xy}[P(i = j|xy) - P(i \neq j|xy)], \tag{4}$$

where $x \in \{\alpha_0, \alpha_1\}, y \in \{\beta_0, \beta_1\}$. The maximal CHSH values are 2 and $2\sqrt{2}$ for LHV models and quantum theory [2, 40], respectively. If $S > 2$, Alice's and Bob's correlation are nonlocal.

The schematic setup, as shown in figure 1, is composed of two parts: the heralded entangled source and the CHSH test. The experiment setup for CHSH test consists of a polarization modulator (PM), a polarization beam splitter (PBS) and two detectors in Alice's side and similarly for Bob. The PM is used to choose different measurement settings. The coincidence of four detectors D_1, D_2, D_3 and D_4 heralds the output of entangled photon pairs. However, because of the inefficiency of the detector, the dark-count and the higher order components of the conventional SPDC source, there are also vacuum state and multi-pair components in the output mode of the heralded entangled source. As for the CHSH test, there are four detection events at Alice's (Bob's) side: double clicks, ±1 click and no click. In order to close the fair-sampling loophole [28, 33], one need to take all the detection events into consideration. One denotes the events that A_H does not click and A_V clicks as

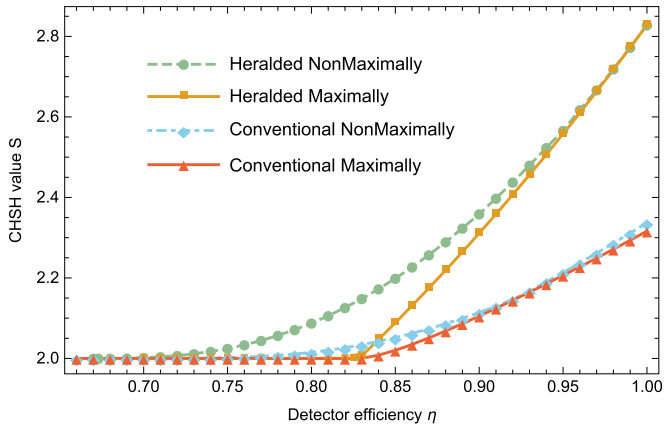

Figure 2. CHSH values S for the heralded entangled source and the conventional SPDC source versus the detector efficiency η. The simulation results are obtained when taking $p_d = 0$ for both the conventional and heralded entangled source. Meanwhile, the transmission coefficient η_{trans} almost equals to 1 for the heralded entangled source. The dashed circle line and the solid quadrate line denote CHSH values for non-maximally and maximally entangled output mode of the heralded entangled source, respectively. The dotted–dashed rhombus line and the solid trilateral line denote CHSH values for non-maximally and maximally entangled output mode of the conventional SPDC source, respectively.

-1, other events are counted as $+1$ for Alice. Also, the events that B_H does not click and B_V clicks are counted as -1, others counted as $+1$ for Bob [39]. To compare with the CHSH test using the conventional SPDC source, one can calculate the CHSH value S when the dark-count rate equals $p_d = 0$ which is chosen according to [39]. At the same time, the transmission coefficient η_{trans} of the BSs in the heralded entangled source approaches to 1. The simulation is cut off at $n = 5$, which is reasonable, because it can be certified through simple calculation that the CHSH value contributed by the component of $n \geqslant 6$ from equation (1) is negligible compared with that contributed by the dark-count events when $p_d \geqslant 10^{-8}$ which is reasonably chosen according to [45, 46].

As shown in figure 2, one can see that the CHSH values for non-maximally entangled output modes are higher than the one for maximally entangled output modes from both the heralded entangled source and the conventional SPDC source. This is because that non-maximally entangled states can tolerate more noises than maximally entangled states [23]. Without considering the system error, the maximal violation for CHSH inequality using the heralded entangled source is 2.828 when $\eta_{\text{trans}} = 0.999\,999$, which is approaching $2\sqrt{2}$ allowed by Tsirelson's bound in quantum theory [40]. This result is significantly higher than 2.35 which is the maximal violation for CHSH inequality using multi-mode emission of the conventional SPDC source even with detector efficiency $\eta = 1$ [39]. The lower bound of detector efficiency for loophole-free CHSH inequality violation using the heralded entangled source approaches 67.3%, and the corresponding CHSH value is $S = 2.000\,01$. As shown in [23], the lower bound for a loophole-free Bell inequality violation is $2/3$ when non-maximally entangled state is adopted. It is shown in equation (C.7) that the fidelity of the output entangled state increases as the transmission coefficient increases. When $\eta_{\text{trans}} \to 1$, one can achieve a lower bound of detector efficiency $\eta \to 2/3$ for CHSH inequality violation using the heralded entangled source.

To match the actual experiment setups, one can take reasonable transmission coefficients η_{trans} and dark-count rate p_d when estimating the CHSH value. Specifically, we provide simulation for the CHSH test with non-maximally and maximally entangled output modes from the heralded entangled source at two different transmission coefficients. The first one is $\eta_{\text{trans}_1} = 0.99$ which is derived from [47]. According to equation (C.6) the preparation probability of entangled pairs approaches 0 when transmission coefficient approaches to 1. The second one is chosen at $\eta_{\text{trans}_2} = 0.9$ to make a tradeoff between the preparation probability and the amounts of violation of CHSH inequality. At the same time, the dark count rate is set to be $p_d = 10^{-6}$ which is derived according to [35].

As shown in figure 3, the CHSH value S at $\eta_{\text{trans}_1} = 0.99$ is higher than that at $\eta_{\text{trans}_2} = 0.9$ for both the maximally and non-maximally entangled output modes at most values of the detection efficiency η. That is because the fidelity of the output entangled state increases as the transmission coefficient increases according to equation (C.7) and entangled states with higher fidelity can achieve better CHSH inequality violation. For the non-maximally entangled output mode, when $\eta_{\text{trans}_1} = 0.99$, the minimal detector efficiency for violating the CHSH inequality is $\eta \approx 80.9\%$. But when $\eta_{\text{trans}_2} = 0.9$, the minimal detector efficiency for violating the CHSH inequality is $\eta \approx 80.3\%$ which is lower. The reason for this counter-intuitive phenomenon is that the dark-count rate in case is big enough to break down the advantage in fidelity of entangled state induced by higher transmission coefficient which will cause lower preparation probability of the heralded entangled source according to equation (C.6). More specifically, as shown in table 1, one can see that the CHSH value S with

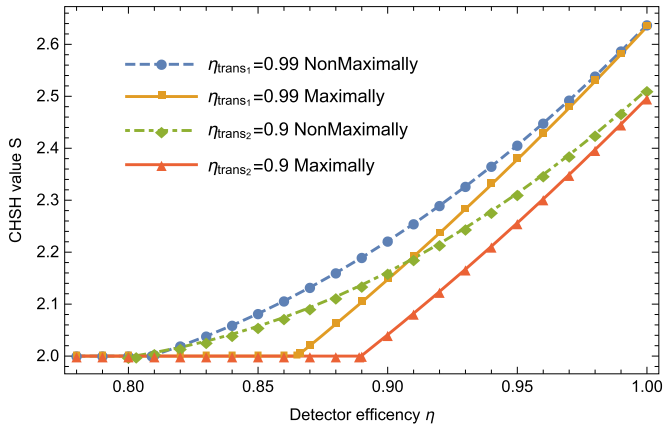

Figure 3. CHSH value S versus detector efficiency η. The dark-count rate is set to be $p_d = 10^{-6}$. The dashed circle line and the solid quadrate line denote CHSH values with $\eta_{trans_1} = 0.99$ for heralded non-maximally entangled output and heralded maximally entangled output mode, respectively. The dotted–dashed rhombus line and the solid trilateral line denote CHSH values with $\eta_{trans_2} = 0.9$ for heralded non-maximally entangled output and heralded maximally entangled output mode, respectively.

Table 1. Comparison for the performance of the CHSH tests with different dark-count rates at $\eta = 80.9\%$[a]. When $p_d = 10^{-6}$, one can see that the CHSH value with transmission efficient $\eta_{trans_1} = 0.99$ is lower than that with $\eta_{trans_2} = 0.9$. While, when $p_d = 10^{-7}$ the CHSH value with transmission efficient $\eta_{trans_1} = 0.99$ is higher than that with $\eta_{trans_2} = 0.9$. Here, g and $\bar{g}$ are the corresponding squeezing parameters of the SPDC source (see appendix B).

η	p_d	η_{trans}	g	$\bar{g}$	α_0	α_1	β_0	β_1	S
80.9%	10^{-6}	0.99	0.0988	0.0456	0.1124	−0.5523	−0.1324	0.5066	2.000 33 (2.000 36)
80.9%	10^{-6}	0.9	0.0579	0.0195	0.0863	−0.4953	−0.0959	0.4731	2.005 86
80.9%	10^{-7}	0.99	0.0564	0.0265	0.2158	−0.5406	−0.1341	0.5252	2.045 89 (2.0648)
80.9%	10^{-7}	0.9	0.0330	0.0111	0.0912	−0.4891	−0.0943	0.4818	2.024 06

Note.

[a] The simulations are implemented with *Wolfram Mathematica* on a standard laptop computer by default accuracy. Due to the round-off of g, $\bar{g}$, α_0, α_1, β_0 and β_1 to four decimal places, there are differences between the presented values of S and the true optimal values which have also been presented in the round brackets.

$\eta_{trans_1} = 0.99$ is higher than that with $\eta_{trans_2} = 0.9$ at $\eta = 80.9\%$ when the dark-count rate is turn down to $p_d = 10^{-7}$. According to the detector efficiency $\eta \approx 82.28\%$ reported in a recent experiment [17], the detector within current technology is enough for loophole-free CHSH tests using the heralded entangled source.

3.2. Loophole-free CH test using heralded entangled source

Among recently reported experimental loophole-free Bell tests [32–37], the CH inequality [3, 23] is employed extensively. In order to make a comparison with the reported results, we propose a CH test scheme using the heralded entangled source and experiment parameters comparable to that in [34]. The CH inequality is of the form [48]

$$J \equiv P_{++}(\alpha_0\beta_0) - P_{+0}(\alpha_0\beta_1) - P_{0+}(\alpha_1\beta_0) - P_{++}(\alpha_1\beta_1) \leqslant 0. \tag{5}$$

The experimental setup for the CH test is similar to the CHSH test in figure 1, except that there is only one detector in Alice's (Bob's) side. As for the CH test, there are only two detection events in Alice's (Bob's) side: click and no click. One counts events that Alice's (Bob's) detector clicks as + and does not click as 0 in the CH test. The trial is repeated enough times to accurately calculate the CH value J. The violation of the CH inequality means that Alice's and Bob's correlation are nonlocal.

As illustrated in figure 4, the corresponding experiment parameters are set to be $p_d = 10^{-7}$ and $\eta_{trans} = 0.95$ without loss of generality. The red X mark denotes the result reported in [34] that $J = 7.27 \times 10^{-6}$ when $\eta = 77.39\%$ (the detector efficiency is taken as a geometric average over Alice's and Bob's detector efficiencies in [34]). The CH value using the heralded entangled source is $J = 9.06 \times 10^{-4}$ which is two order of magnitude better than that reported in [34] at the same detector efficiency. As presented in figure 3, better violations can be achieved for the CHSH test by adjusting the transmission coefficients of the BSs in the heralded entangled source because one can achieve a higher fidelity of the entangled source by adjusting η_{trans} according to equation (C.7). It should be noted that one can also obtain even better results by adjusting the transmission coefficients of the BSs in the heralded entangled source for the same reason.

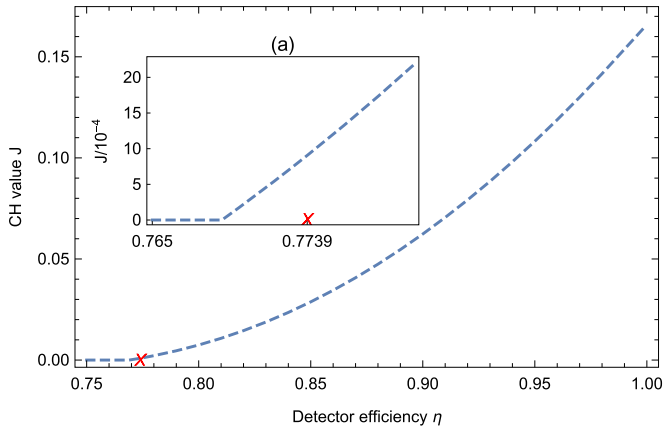

Figure 4. CH value J versus detector efficiency η. The simulation result is obtained with $p_d = 10^{-7}$ and $\eta_{\text{trans}} = 0.95$. The dashed line denotes CH values using the heralded entangled source. The X mark denotes the result of [34] that $J = 7.27 \times 10^{-6}$ when $\eta = 77.39\%$. The inset figure (a) is a zoom on $\eta \in [0.765, 0.78]$.

4. Application: DI-QKD using heralded entangled source

As one of the most promising applications of Bell non-locality, the DI-QKD provides a way that Alice and Bob can conduct secure communication without trusting the devices [6, 7, 10, 11]. The schematic setup for DI-QKD protocol is similar with that for CHSH test shown in figure 1, except that Alice's measurement setting choices is $\{\alpha_0, \alpha_1, \alpha_2\}$. The DI-QKD protocol runs as follows. Alice and Bob share entangled photon pairs from a third party, who can be untrustworthy. Alice randomly chooses a measurement x from measurement setting choices $\{\alpha_0, \alpha_1, \alpha_2\}$ to measure the particle in her side, and similarly for Bob with measurement setting choices $y \in \{\beta_0, \beta_1\}$, and the trial is repeated many times. After their measurements, Alice and Bob obtain two sequences of measurement results. They use the measurement results generated by $x \in \{\alpha_0, \alpha_1\}$ and $y \in \{\beta_0, \beta_1\}$ to estimate the loophole-free CHSH value S. The measurement setting α_2 is set to be the same with β_0, and the measurement results generated by α_2 and β_0 are used to estimate the quantum bit error rate Q. The key generation rate R is bounded by [6, 7]

$$R \geqslant 1 - h(Q) - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right), \tag{6}$$

where $h(x) = -x \log_2 x - (1 - x)\log_2(1 - x)$ is the binary entropy, $Q = P(i \neq j|\alpha_2\beta_0)$ is the probability that Alice and Bob obtain different measurement results when they choose measurement settings α_2 and β_0, respectively.

Let us compare the DI-QKD key generation rate using the non-maximally entangled output mode from the heralded entangled source with that using the non-maximally entangled output mode from the conventional SPDC source with $p_d = 0$. The measurement setting choices $\{\alpha_0, \alpha_1, \alpha_2\}$ and $\{\beta_0, \beta_1\}$ are determined by optimizing the CHSH value S at different given parameters. As shown in figure 5, the blue line denotes key generation rate using non-maximally entangled photon pairs from the heralded entangled source when the transmission coefficient η_{trans} approaches to 1. The yellow lower line denotes key generation rate with non-maximally entangled photon pairs from the conventional SPDC source.

As a result, a lower bound of $\eta_L \approx 91\%$ is obtained with the heralded entangled source, and further calculation shows that this result is close to the one using non-maximally entangled state as equation (2). The lower bound is better than $\eta_{L'} \approx 95.3\%$ which is the lower bound using the conventional SPDC source. At the same time, the key generation rate using the heralded entangled source is significantly higher than that using the conventional SPDC source. When $\eta = 1$, we realize a 2.62 times improvement in key generation rate compare with the DI-QKD setup with conventional SPDC source. The previous work shows that the detector efficiency should be $\eta \geqslant 92.4\%$ to conduct a DI-QKD protocol [7], we illustrate that it is possible to lower significantly the requirement of the efficiency of detectors in a DI-QKD protocol.

5. Discussions and conclusions

In conclusion, a new loophole-free Bell test scheme based on the heralded entangled source has been presented. We demonstrate that the CHSH test using the heralded entangled source can dramatically surpass the one using

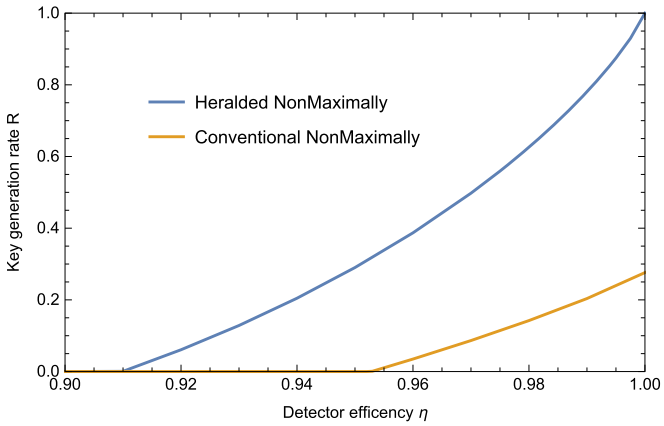

Figure 5. DI-QKD key generation rate R versus detector efficiency η. This DI-QKD protocol simulation is conducted with $p_d = 0$. The blue line denotes key generation rate using non-maximally entangled photon pairs from the heralded entangled source when the transmission coefficient η_{trans} approaches to 1. The yellow lower line denotes key generation rate using non-maximally entangled photon pairs from the conventional SPDC source.

the conventional SPDC source, for both non-maximally entangled and maximally entangled output modes. The maximal violation of CHSH inequality using the heralded entangled source can almost approach $2\sqrt{2}$ which is bounded by quantum theory. It is also shown that the CH inequality violation using the heralded entangled source can be two orders of magnitude better compared with that reported in [34] at typical experiment parameters. Being one of the most promising applications of Bell non-locality, we show that it is possible to lower significantly the requirement of the efficiency of detectors in a DI-QKD protocol. At the same time, the DI-QKD key generation rate using the heralded entangled source is much higher than the one using the conventional SPDC source with a more broad range. After considering the experimentally reasonable parameters, it turns out that the detector within current technology is feasible for loophole-free CHSH tests by implementing this scheme. With the merit of lower requirements than conventional SPDC source, we anticipant that our proposals may facilitate ongoing Bell test experiments and various device-independent quantum information tasks.

Acknowledgments

We acknowledge V Caprara Vivoli, Qiang Zhang, Yu-Ao Chen, Xiao-Hui Bao and Jun Zhang for helpful discussion. This work has been supported by the Chinese Academy of Science, the National Fundamental Research Program, National Key Research and Development Program of China (2018YFB0504303), the National Natural Science Foundation of China (Grants No. 11575174, No. 11374287, No. 11574297, and No. 61771443), the Fundamental Research Funds for the Central Universities (WK2340000083), as well as the Anhui Initiative in Quantum Information Technologies.

Appendix A. Modeling the channel and detection

We consider the non-photon-number-resolving detectors with overall detection efficiency η_0 which includes the detector efficiency and internal transmission efficiency. The fiber channel loss is $\eta_l = 10^{-\frac{\xi l}{10}}$ with a loss rate ξ measured in dB km^{-1}, and l represent the distance of the channel. Without loss of generality, the channel and detection can be modeled as a beam splitter (BS) with transmission rate η and a perfect non-photon-number-resolving single photon detector

$$\eta = \eta_0 \cdot \eta_l. \tag{A.1}$$

Now, combining the consideration of the dark-count rate p_d, the no-click probability P_{NC} and the click probability P_{C} of a non-photon-number-resolving detector for incoming m photons is

$$\begin{aligned} P_{\text{NC}}(m) &= (1 - p_d)(1 - \eta)^m, \\ P_{\text{C}}(m) &= 1 - P_{\text{NC}}(m), \end{aligned} \tag{A.2}$$

where η is the transmission rate of the BS in the above model of the detection and channel. Without causing misunderstanding, we will directly call η the detection efficiency of a non-photon-number-resolving detector in the main text and other parts of the appendix.

Appendix B. The conventional polarization-entangled SPDC source

The photon pairs generated by SPDC can be labeled by creation operators $\hat{a}_H^\dagger$, $\hat{a}_V^\dagger$, $\hat{b}_H^\dagger$ and $\hat{b}_V^\dagger$ [39, 41], where $\{H, V\}$ is an orthogonal polarizing basis, a and b are spacial modes of down-conversion photons. The Hamiltonian of the down-conversion process is $\hat{H} = \mathrm{i}[\chi(\hat{a}_H^\dagger \hat{b}_V^\dagger - \hat{a}_H \hat{b}_V) - \bar{\chi}(\hat{a}_V^\dagger \hat{b}_H^\dagger - \hat{a}_V \hat{b}_H)]$, where only the polarization mode is considered, χ and $\bar{\chi}$ are proportional to the nonlinear susceptibility of the crystal and to the power of the pump. The output mode of conventional SPDC source has the form [41, 44]

$$\begin{aligned}|\Psi\rangle &= \frac{1}{C_g C_{\bar{g}}} \mathrm{e}^{T_{\bar{g}} \hat{a}_H^\dagger \hat{b}_V^\dagger - T_{\bar{g}} \hat{a}_V^\dagger \hat{b}_H^\dagger} |\mathrm{vac}\rangle \\ &= \sum_{n=0}^{\infty} \lambda_n |\psi_n\rangle, \end{aligned} \tag{B.1}$$

where $g = \chi t$, $\bar{g} = \bar{\chi} t$ are the corresponding squeezing parameters, t is the interaction time, $T_g = \tanh(g)$, $T_{\bar{g}} = \tanh(\bar{g})$, $C_g = \cosh(g)$, $C_{\bar{g}} = \cosh(\bar{g})$, $\lambda_n = \frac{k_n T_g^n}{C_g C_{\bar{g}}}$ is the probability amplitude of the nth order of the output mode of the SPDC source, $k_n = \sqrt{\sum_{m=0}^{n} r^{2(n-m)}}$, $r = \frac{T_g}{T_{\bar{g}}}$ and $|\mathrm{vac}\rangle$ is the vacuum state. The corresponding wave function for n pairs of photons is

$$\begin{aligned}|\psi_n\rangle &= \frac{1}{n! k_n} (r \hat{a}_H^\dagger \hat{b}_V^\dagger - \hat{a}_V^\dagger \hat{b}_H^\dagger)^n |\mathrm{vac}\rangle \\ &= \frac{1}{k_n} \sum_{m=0}^{n} r^{(n-m)} (-1)^m |n-m, m; m, n-m\rangle, \end{aligned} \tag{B.2}$$

where $|n-m, m; m, n-m\rangle$ is in the form of Fock state $|n_{a_H}, n_{a_V}; n_{b_H}, n_{b_V}\rangle$ with corresponding photon numbers for different output paths. For $n = 1$, the output mode is an entangled state

$$\begin{aligned}|\psi_1\rangle &= \frac{1}{\sqrt{r^2+1}} (r|1, 0; 0, 1\rangle - |0, 1; 1, 0\rangle)_{a_H, a_V; b_H, b_V} \\ &= \frac{1}{\sqrt{r^2+1}} (r|HV\rangle - |VH\rangle)_{ab}. \end{aligned} \tag{B.3}$$

When $r = 1$, this state reduces to the maximally entangled state

$$|\psi_1'\rangle = \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle)_{ab}. \tag{B.4}$$

For $n = 0$ and $n \geqslant 2$, the output mode are vacuum and multi-pair states. For example, when $n = 6$, the corresponding output mode $|\psi_6\rangle$ contains 6 pairs of photon and the corresponding probability $|\lambda_6|^2 = 2.247\,98 \times 10^{-11}$ with $g \sim 0.106$ and $g \sim 0.115$ which are chosen from [39].

Appendix C. The heralded polarization-entangled source

The heralded entangled source consists of a conventional SPDC source and a linear optical part which is used to herald generations of entangled pairs. The coincidence of four detectors D_1, D_2, D_3 and D_4 at the end of paths after two PBSs indicates a successful preparation of one pair of entanglement photons.

The schematic setup is shown in figure C1. The BS after the SPDC source are non-polarizing, and the corresponding transmission coefficient is $\eta_{\mathrm{trans}} = \cos^2\theta$. We can model the BSs as [41]

$$\begin{aligned}\hat{a}_H^\dagger &= \hat{c}_H^\dagger \cos\theta + \hat{e}_H^\dagger \sin\theta, \\ \hat{a}_V^\dagger &= \hat{c}_V^\dagger \cos\theta + \hat{e}_V^\dagger \sin\theta, \\ \hat{b}_H^\dagger &= \hat{d}_H^\dagger \cos\theta + (\hat{f}_+^\dagger + \hat{f}_-^\dagger) \sin\theta/\sqrt{2}, \\ \hat{b}_V^\dagger &= \hat{d}_V^\dagger \cos\theta + (\hat{f}_+^\dagger - \hat{f}_-^\dagger) \sin\theta/\sqrt{2}, \end{aligned} \tag{C.1}$$

where a, b, c, d, e and f label the paths of beams, $\hat{f}_H^\dagger = (\hat{f}_+^\dagger + \hat{f}_-^\dagger)/\sqrt{2}$ and $\hat{f}_V^\dagger = (\hat{f}_+^\dagger - \hat{f}_-^\dagger)/\sqrt{2}$ model the half wave plates along the f beam, $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$, and $\{+, -\}$ is an orthogonal polarizing basis.

As analyzed in [41], $n = 3$ is the lowest order that contributes to the coincidence of four detectors D_1, D_2, D_3 and D_4 of the SPDC source, and the corresponding output mode is an entangled state

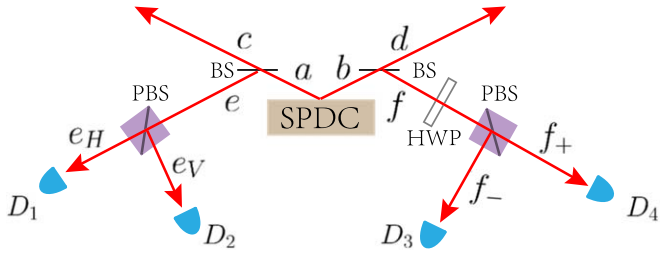

Figure C1. Schematic setup for the heralded entangled source. a, b, c, d, e and f label the paths of beams. $D_{1(2)}$ and $D_{3(4)}$ label the corresponding non-photon-number-resolving detectors. BS: non-polarization beam splitter; HWP: half-wave plate; PBS: polarization beam splitter; SPDC: spontaneous parametric down-conversion source.

$$|\phi_r\rangle = \frac{1}{\sqrt{r^2+1}}(r|HH\rangle + |VV\rangle). \tag{C.2}$$

When $r = 1$, it reduces to the maximally entangled state

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle). \tag{C.3}$$

Specifically, according to the equation (B.2), the corresponding output mode of the conventional SPDC source for $n = 3$ is

$$|\psi_3\rangle = \frac{1}{3!\sqrt{1+r^2+r^4+r^6}}(r\hat{a}_H^\dagger \hat{b}_V^\dagger - \hat{a}_V^\dagger \hat{b}_H^\dagger)^3|\text{vac}\rangle. \tag{C.4}$$

Through direct calculation, the density matrix of the heralding output state for the coincidence of four herald non-photon-number-resolving detectors is

$$\begin{aligned}\hat{\rho} = \frac{r^2\eta^4(1-\eta_{\text{trans}})^4}{1+r^2+r^4+r^6}\Big[&(1+r^2)\eta_{\text{trans}}^2|\phi_r\rangle\langle\phi_r| + \frac{1}{2}(2-\eta)\eta_{\text{trans}}(1-\eta_{\text{trans}})(|0,0;0,1\rangle\langle 0,0;0,1| \\ &+ r^2|0,0;1,0\rangle\langle 0,0;1,0| + |0,1;0,0\rangle\langle 0,1;0,0| + r^2|1,0;0,0\rangle\langle 1,0;0,0|) \\ &+ \frac{(1+r^2)}{4}(2-\eta)^2(1-\eta_{\text{trans}})^2|\text{vac}\rangle\langle\text{vac}|\Big].\end{aligned} \tag{C.5}$$

The probability of the coincidence of the four heralding non-photon-number-resolving events is

$$P_{\text{co}} = \text{Tr}[\hat{\rho}] = \frac{r^2}{1+r^4}\eta^4(1-\eta_{\text{trans}})^4\left[1-\frac{1}{2}\eta(1-\eta_{\text{trans}})\right]^2. \tag{C.6}$$

The fidelity of the heralded entangled pair is

$$F = \sqrt{\frac{\langle\phi_r|\hat{\rho}|\phi_r\rangle}{\text{Tr}[\hat{\rho}]}} = \frac{\eta_{\text{trans}}}{1-\frac{1}{2}\eta(1-\eta_{\text{trans}})}. \tag{C.7}$$

The correlation between the coincidence probability P_{co} and fidelity F are similar with that in [39] except that the detectors are non-photon-number-resolving here.

Appendix D. Calculating the probability distribution of the detection events for the CHSH test

Alice and Bob choose their measurement settings before the detection of the photons in each trial as [39]

$$\begin{aligned}\hat{c}_H^\dagger &= \cos\alpha\,\hat{A}_H^\dagger + e^{i\phi_\alpha}\sin\alpha\,\hat{A}_V^\dagger, \\ \hat{c}_V^\dagger &= e^{-i\phi_\alpha}\sin\alpha\,\hat{A}_H^\dagger - \cos\alpha\,\hat{A}_V^\dagger, \\ \hat{d}_H^\dagger &= \cos\beta\,\hat{B}_H^\dagger + e^{i\phi_\beta}\sin\beta\,\hat{B}_V^\dagger, \\ \hat{d}_V^\dagger &= e^{-i\phi_\beta}\sin\beta\,\hat{B}_H^\dagger - \cos\beta\,\hat{B}_V^\dagger.\end{aligned} \tag{D.1}$$

Combing equations (B.1), (B.2), (C.1) and (D.1), the output mode of the conventional SPDC source can be expressed in the Fock basis as

$$|\Psi\rangle = \sum_{m_{e_H},\cdots,m_{B_V}} R_{m_{e_H},\cdots,m_{B_V}} \times |m_{e_H}, m_{e_V}; m_{f_+}, m_{f_-}; m_{A_H}, m_{A_V}; m_{B_H}, m_{B_V}\rangle, \tag{D.2}$$

where $m_{e_H},\cdots,m_{B_V}$ are the numbers of photon transmitted in path modes $e_H, \cdots, B_V$. $R_{m_{e_H},\cdots,m_{B_V}}$ is the normalized probability amplitude of the corresponding component of the state expressed in the Fock basis.

To calculate the CHSH value, we need to calculate the probability distribution $P(ij|xy)$ for $i, j \in \{+1, -1\}$, $x \in \{\alpha_0, \alpha_1\}$ and $y \in \{\beta_0, \beta_1\}$ in equation (4). For the chosen measurement settings x and y, there are four detection events at Alice's (Bob's) side: double clicks, ± 1 click and no click. In order to close the fair-sampling loophole, one need to take all the detection events into consideration. without loss of generality, one denotes the events that A_H does not click and A_V clicks as -1, other events are counted as $+1$ for Alice. Also, the events that B_H does not click and B_V clicks are counted as -1, others counted as $+1$ for Bob [39]. Thus, according to equations (A.2) and (D.2), the corresponding probability distributions $P(ij|xy)$ are expressed as

$$\begin{aligned} P(-1\ -\ 1|xy) = & \sum_{m_{e_H},\cdots,m_{B_V}} |R_{m_{e_H},\cdots,m_{B_V}}|^2 \cdot P_{\mathrm{C}}(m_{e_H}) P_{\mathrm{C}}(m_{e_V}) P_{\mathrm{C}}(m_{f_+}) P_{\mathrm{C}}(m_{f_-}) \\ & \cdot P_{\mathrm{NC}}(m_{A_H}) P_{\mathrm{C}}(m_{A_V}) P_{\mathrm{NC}}(m_{B_H}) P_{\mathrm{C}}(m_{B_V}), \end{aligned} \tag{D.3}$$

$$\begin{aligned} P(+1\ -\ 1|xy) = & \sum_{m_{e_H},\cdots,m_{B_V}} |R_{m_{e_H},\cdots,m_{B_V}}|^2 \cdot P_{\mathrm{C}}(m_{e_H}) P_{\mathrm{C}}(m_{e_V}) P_{\mathrm{C}}(m_{f_+}) P_{\mathrm{C}}(m_{f_-}) \\ & \cdot [1 - P_{\mathrm{NC}}(m_{A_H}) P_{\mathrm{C}}(m_{A_V})] P_{\mathrm{NC}}(m_{B_H}) P_{\mathrm{C}}(m_{B_V}), \end{aligned} \tag{D.4}$$

$$\begin{aligned} P(-1\ +\ 1|xy) = & \sum_{m_{e_H},\cdots,m_{B_V}} |R_{m_{e_H},\cdots,m_{B_V}}|^2 \cdot P_{\mathrm{C}}(m_{e_H}) P_{\mathrm{C}}(m_{e_V}) P_{\mathrm{C}}(m_{f_+}) P_{\mathrm{C}}(m_{f_-}) \\ & \cdot P_{\mathrm{NC}}(m_{A_H}) P_{\mathrm{C}}(m_{A_V}) [1 - P_{\mathrm{NC}}(m_{B_H}) P_{\mathrm{C}}(m_{B_V})], \end{aligned} \tag{D.5}$$

$$\begin{aligned} P(+1\ +\ 1|xy) = & \sum_{m_{e_H},\cdots,m_{B_V}} |R_{m_{e_H},\cdots,m_{B_V}}|^2 \cdot P_{\mathrm{C}}(m_{e_H}) P_{\mathrm{C}}(m_{e_V}) P_{\mathrm{C}}(m_{f_+}) P_{\mathrm{C}}(m_{f_-}) \\ & \cdot [1 - P_{\mathrm{NC}}(m_{A_H}) P_{\mathrm{C}}(m_{A_V})][1 - P_{\mathrm{NC}}(m_{B_H}) P_{\mathrm{C}}(m_{B_V})]. \end{aligned} \tag{D.6}$$

Here, for the sake of simplicity and without loss of generality, we have set the detection efficiency η to be the same for all eight detectors. From equations (B.1), (D.2) and (D.3) to (D.6), one can optimize the CHSH value over the squeezing parameters g and $\bar{g}$, measurement settings $\{\alpha_0, \alpha_1\}$ and $\{\beta_0, \beta_1\}$ for given transmission efficiency η_{trans}, detection efficiencies of the detectors and the dark-count rate p_d.

ORCID iDs

Feihu Xu https://orcid.org/0000-0002-1643-225X
Kai Chen https://orcid.org/0000-0001-9833-8197

References

[1] Bell J *et al* 1964 *Phys.* **1** 195
[2] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880
[3] Clauser J F and Horne M A 1974 *Phys. Rev.* D **10** 526
[4] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 *Rev. Mod. Phys.* **86** 419–78
[5] Einstein A, Podolsky B and Rosen N 1935 *Phys. Rev.* **47** 777
[6] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[7] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021
[8] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
[9] Curty M and Moroder T 2011 *Phys. Rev.* A **84** 010304
[10] Barrett J, Colbeck R and Kent A 2012 *Phys. Rev.* A **86** 062326
[11] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[12] Pironio S *et al* 2010 *Nature* **464** 1021
[13] Acín A, Massar S and Pironio S 2012 *Phys. Rev. Lett.* **108** 100402
[14] Pironio S and Massar S 2013 *Phys. Rev.* A **87** 012336
[15] Vivoli V C, Sekatski P, Bancal J D, Lim C C W, Martin A, Thew R T, Zbinden H, Gisin N and Sangouard N 2015 *New J. Phys.* **17** 023023
[16] Ma X, Yuan X, Cao Z, Qi B and Zhang Z 2016 *NPJ Quantum Inf.* **2** 16021
[17] Shen L *et al* 2018 *Phys. Rev. Lett.* **121** 150402
[18] Liu Y *et al* 2018 *Phys. Rev. Lett.* **120** 010503
[19] Bierhorst P *et al* 2018 *Nature* **556** 223
[20] Liu Y *et al* 2018 *Nature* **562** 548
[21] Xu F *et al* 2019 arXiv:1903.09051
[22] Herrero-Collantes M and Garcia-Escartin J C 2017 *Rev. Mod. Phys.* **89** 015004
[23] Eberhard P H 1993 *Phys. Rev.* A **47** R747–50
[24] Collins D, Gisin N, Linden N, Massar S and Popescu S 2002 *Phys. Rev. Lett.* **88** 040404
[25] Śliwa C 2003 *Phys. Lett.* A **317** 165–8
[26] Collins D and Gisin N 2004 *J. Phys. A: Math. Gen.* **37** 1775
[27] Barrett J, Kent A and Pironio S 2006 *Phys. Rev. Lett.* **97** 170409

[28] Kofler J, Giustina M, Larsson J Å and Mitchell M W 2016 *Phys. Rev.* A **93** 032115
[29] Scheidl T *et al* 2010 *Proc. Natl Acad. Sci.* **107** 19708–13
[30] Pearle P M 1970 *Phys. Rev.* D **2** 1418
[31] Brunner N, Gisin N, Scarani V and Simon C 2007 *Phys. Rev. Lett.* **98** 220403
[32] Christensen B *et al* 2013 *Phys. Rev. Lett.* **111** 130406
[33] Giustina M *et al* 2013 *Nature* **497** 227
[34] Giustina M *et al* 2015 *Phys. Rev. Lett.* **115** 250401
[35] Shalm L K *et al* 2015 *Phys. Rev. Lett.* **115** 250402
[36] Hensen B *et al* 2015 *Nature* **526** 682–6
[37] Rosenfeld W, Burchardt D, Garthoff R, Redeker K, Ortegel N, Rau M and Weinfurter H 2017 *Phys. Rev. Lett.* **119** 010402
[38] Kwiat P 1995 *Phys. Rev. Lett.* **75** 4337
[39] Caprara Vivoli V, Sekatski P, Bancal J D, Lim C C W, Christensen B G, Martin A, Thew R T, Zbinden H, Gisin N and Sangouard N 2015 *Phys. Rev.* A **91** 012107
[40] Tsirelson B 1993 *Hadronic J. Suppl.* **8** 329–45
[41] Śliwa C and Banaszek K 2003 *Phys. Rev.* A **67** 030101
[42] Wagenknecht C, Li C M, Reingruber A, Bao X H, Goebel A, Chen Y A, Zhang Q, Chen K and Pan J W 2010 *Nat. Photon.* **4** 549
[43] Barz S, Cronenberg G, Zeilinger A and Walther P 2010 *Nat. Photon.* **4** 553
[44] Lamas-Linares A, Howell J C and Bouwmeester D 2001 *Nature* **412** 887
[45] Marsili F *et al* 2013 *Nat. Photon.* **7** 210
[46] Zhang W, You L, Li H, Huang J, Lv C, Zhang L, Liu X, Wu J, Wang Z and Xie X 2017 *Sci. China Phy., Mech. Astron.* **60** 120314
[47] Koike S, Takahashi H, Yonezawa H, Takei N, Braunstein S L, Aoki T and Furusawa A 2006 *Phys. Rev. Lett.* **96** 060504
[48] Bierhorst P 2015 *J. Phys. A: Math. Theor.* **48** 195302