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

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

Comparing different approaches for generating random numbers device-independently using a photon pair source

To cite this article: V Caprara Vivoli *et al* 2015 *New J. Phys.* **17** 023023

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
17 September 2014

REVISED
15 December 2014

ACCEPTED FOR PUBLICATION
15 January 2015

PUBLISHED
10 February 2015

PAPER

Comparing different approaches for generating random numbers device-independently using a photon pair source

V Caprara Vivoli[1], P Sekatski[2], J-D Bancal[3], C C W Lim[1], A Martin[1], R T Thew[1], H Zbinden[1], N Gisin[1] and N Sangouard[4]

[1] Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland
[2] Institut for Theoretische Physik, Universitat of Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria
[3] Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore
[4] Department of Physics, University of Basel, CH-4056 Basel, Switzerland

E-mail: valentina.caprara@unige.ch

Keywords: non-locality, random numbers, photon pair source

Abstract

What is the most efficient way to generate random numbers device-independently using a photon pair source based on spontaneous parametric down conversion? We consider this question by comparing two implementations of a detection-loophole-free Bell test. In particular, we study in detail a scenario where a source is used to herald path-entangled states, i.e. entanglement between two spatial modes sharing a single photon and where non-locality is revealed using photon counting preceded by small displacement operations. We start by giving a theoretical description of such a measurement. We then show how to optimize the Bell–CHSH violation through a non-perturbative calculation, taking the main experimental imperfections into account. We finally bound the amount of randomness that can be extracted and compare it to the one obtained with the conventional scenario using photon pairs entangled e.g. in polarization and analyzed through photon counting. While the former requires higher overall detection efficiencies, it is far more efficient in terms of the entropy per experimental run and under reasonable assumptions, it provides higher random bit rates.

1. Introduction

In the last decades, the idea of using the randomness present in quantum phenomena to create random number strings has been pushed forward [1–3]. Among the quantum techniques that are envisaged to expand a given random bit string, those based on a Bell test [4–6], the so-called device-independent quantum random number generators (DI-QRNG), are very attractive because they are based on a few assumptions that are relatively easy to check in real time. The price to pay is to realize a Bell test without the detection loophole. The detection loophole has been addressed in several experiments including single ions [7, 8] and single atoms [9] and very recently, using photon pair sources [10, 11]. The latter has several advantages in practice in that it is much less restrictive in terms of wavelength and bandwidth than atoms. It further has the advantage of simple implementation since $\chi^{(2)}$ nonlinear crystals are well integrated devices, commercially available and operating at room temperature. The bottleneck of photonic experiments is the detector inefficiency, but given recent improvements [12–15], setups based on spontaneous parametric down conversion (SPDC) sources are attracting more and more attention, including for their commercial perspectives.

The conventional setup, used e.g. in the experiments [10, 11], is shown in figure 1(A). A SPDC source produces photon pairs entangled e.g. in polarization. The photons are then analyzed by a set of wave plates and non-photon number resolving (NPNR) detectors[5]. Importantly, it has been realized recently [16] that the maximal CHSH–Bell violation [17] that can be reached in this scenario is intrinsically limited by the characteristics of the source, i.e. by the presence of vacuum and multiple photon pairs. As shown in [4], the

[5] Note that TES detectors are capable of number resolution. Nevertheless, this capability was not used in [10, 11].

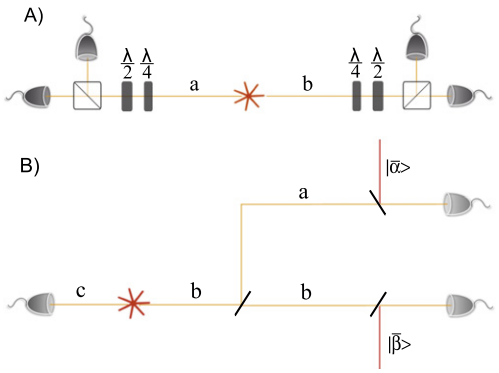

Figure 1. Scheme of two possible implementations of a Bell test using a photon pair source. (A) A source (star) based on SPDC is excited e.g. by a pulsed pump and produce photon pairs entangled e.g. in polarization. The photons are emitted in correlated spatial modes a (b). Each of them might include several temporal/frequency/spatial modes a_k–b_k. The photons emitted in a (b) are sent to Alice's (Bob's) location where they are projected along an arbitrary direction of the Bloch sphere using a set of wave-plates, a polarization beam splitter and two detectors. (B) A source (star) based on SPDC produces photon pairs. We assume that in this scenario the emission is mono-mode. The detection of one photon thus heralds the creation of its twin in a pure state. The latter is sent through a beam splitter. This leads to an entangled state between the two paths a and b. The state of each path is displaced in the phase space using an unbalanced beamsplitter and a coherent state, before being detected though photon counting techniques. The detectors are assumed to be non-photon number resolving with non-unit efficiency.

observed CHSH violation can be used to quantify the amount of extractable randomness in the experimental data. That is, the min-entropy of the data is lower bounded by a function monotonically increasing in the observed CHSH violation. A reduction in the violation thus implies a reduction in the amount of extractable randomness. This raises the question of whether other scenarios involving similar resources could provide larger Bell violations and hence would be more suited for DI-QRNG.

An alternative scenario for Bell test with photons has been proposed by Banaszek and Wodkiewicz in 1998 [18] (see also related theoretical investigations [19–23]) leading to a proof of principle experiment in 2004 [24]. The corresponding implementation using a SPDC source is shown in figure 1(B). A nonlinear crystal is pumped by a pulsed laser with an intensity carefully tuned to create a pair of photons with a small probability in modes b and c. A detection in c, even with an inefficient NPNR detector, heralds the creation of its twin photon in b. The latter is subsequently sent through a beam splitter, entangling the two output spatial modes a and b. Each of these modes is then analyzed through photon counting preceded by small displacements in phase space. Such a displacement is easily implemented in practice, using an unbalanced beamsplitter and a coherent state. In the subspace with at most one photon $\{|0\rangle, |1\rangle\}$, this measurement corresponds to a noisy qubit measurement whose direction in the Bloch sphere depends on the size of the displacement, as detailed below. By choosing the appropriate settings and by taking the events 'click' and 'no-click' as binary outputs of a Bell test, a CHSH–Bell value of $\approx$2.69 can be obtained with a state of the form $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ [20, 21]. However, it was not previously clear what the maximum violation could be in a realistic scenario involving a SPDC source, non-unit efficiency and noisy detectors. Here we present such an analysis with the aim of establishing the best experimental setup for DI-QRNG. More precisely, we start by providing a detailed theoretical analysis of this measurement involving photon counting preceded by a small displacement operation. We then show how to calculate the Bell correlations in a non-perturbative way in the scenario presented in figure 1(B) that we call 'spatial entanglement' in the rest of the paper. We then optimize the CHSH violation for a given detection efficiency η over the squeezing parameter, the displacement amplitudes, and the splitting ratio of the beam splitter. Lastly we calculate the min entropy and the rate of random bits that can be extracted in this setup. We compare them to the conventional case where entangled pairs are detected by photon counting (see figure 1(A)). We show that while the scenario based on spatial entanglement requires higher overall detection efficiencies, it is preferable to the two photon case regarding the min entropy and, under reasonable assumptions, regarding the rate of random bits as well.

2. Measurement analysis

In this section, we provide a detailed analysis of the measurement device used in the scenario based on spatial entanglement. We consider a NPNR detector of efficiency η preceded by a displacement $\alpha = |\alpha|e^{i\delta}$. The no click/click events are associated to two elements of a POVM $\{P_0, P_c\}$ which satisfy $P_0 + P_c = \mathbb{1}$. The no-click event of our NPNR detector is described by the operator $(1-\eta)^{a^\dagger a}$. Taking the displacement into account, one gets

$P_0 = \mathcal{D}^\dagger(\alpha)(1-\eta)^{a^\dagger a}\mathcal{D}(\alpha)$. To gain insight on this measurement, let us restrict P_0 to the Hilbert space spanned by $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ where it takes the following matrix form

$$P_0 = \begin{pmatrix} e^{-\eta|\alpha|^2} & -\eta\,\alpha^* e^{-\eta|\alpha|^2} \\ -\eta\,\alpha e^{-\eta|\alpha|^2} & \left(1-\eta+\eta^2|\alpha|^2\right)e^{-\eta|\alpha|^2} \end{pmatrix}. \tag{1}$$

Let us recall that $P_c = \mathbb{1} - P_0$. For non-unit efficiency $\eta < 1$, the POVM $\{P_0,\ P_c\}$ is not extremal [25]

$$\left\{P_0,\ P_c\right\} = \mu\left\{\Pi_{\vec{n}},\ \Pi_{-\vec{n}}\right\} + \left(1-\mu\right)\left\{r_0\mathbb{1},\ r_c\mathbb{1}\right\}. \tag{2}$$

This means that this measurement corresponds to a projective measurement in the direction

$$\vec{n} \propto \begin{pmatrix} -e^{-\eta|\alpha|^2}\,|\alpha|\,\eta\,\cos\left(\delta\right) \\ e^{-\eta|\alpha|^2}\,|\alpha|\,\eta\,\sin\left(\delta\right) \\ \frac{1}{2}e^{-\eta|\alpha|^2}\eta\left(1-|\alpha|^2\eta\right) \end{pmatrix}$$

on the Bloch sphere with probability

$$\mu = \sqrt{\eta^2 e^{-2|\alpha|^2\eta}\left(|\alpha|^2\left(|\alpha|^2\eta^2 - 2\eta + 4\right) + 1\right)}.$$

With the remaining probability $(1-\mu)$, the output of the measurement is given randomly (regardless of the input state) accordingly to the distribution $\{r_0,\ r_c\}$ where

$$r_0 = \frac{1}{2} \times \frac{\frac{\eta\left(|\alpha|^2\eta - 1\right) + 2}{\sqrt{\eta^2\left(|\alpha|^2\left(\eta\left(|\alpha|^2\eta - 2\right) + 4\right) + 1\right)}} - 1}{\frac{e^{|\alpha|^2\eta}}{\sqrt{\eta^2\left(|\alpha|^2\left(\eta\left(|\alpha|^2\eta - 2\right) + 4\right) + 1\right)}} - 1} \tag{3}$$

and $r_c = 1 - r_0$. As an example, consider the case without displacement $\alpha = 0$. The previous POVM reduces to

$$\left\{P_0,\ P_c\right\} = \eta\left\{\Pi_0,\ \Pi_1\right\} + \left(1-\eta\right)\left\{\mathbb{1},\ 0\right\} \tag{4}$$

i.e. it corresponds to a projective measurement in the direction z with the probability η and with the remaining probability $(1-\eta)$, a no-click event occurs regardless of the input state.

Note that the phase term of the displacement $e^{i\delta}$ affects the polar angle of $\vec{n}$ only. For simplicity, we consider the case $\alpha = |\alpha|$, where the direction of the measurement lays in the x–z plane of the Bloch sphere. We further focus on the projective part of the POVM $\mu\ \{\Pi_{\vec{n}},\ \Pi_{-\vec{n}}\}$ and we look at the direction and length of the corresponding vector $\mu\vec{n}$ on the Bloch sphere. The result is shown in figure 2. For $\eta = 1$ and $\alpha = 0$, this vector is directed in the z direction and has a unit length. The measurement device thus performs a projection along z. When α increases, the vector starts to rotate toward x while its length reduces. For non-unit efficiencies, the vector is shorter and it also rotates toward x when α increases. Surprisingly, we remark that the vector length increases with α (before it drops to zero), i.e. the 'effective detection efficiency' of the measurement setup μ gets larger than the intrinsic efficiency of the detector itself η.

3. Exact derivation of Bell–CHSH correlators

The purpose of this section is to derive the exact expression of the CHSH–Bell correlators in the case of spatial entanglement (see figure 1(B)). We first focus on the density matrix ρ_h of b resulting from a detection in c. The state created by the SPDC source is given by $|\psi\rangle = \sqrt{1-T_g^2}\sum_n \frac{T_g^n}{n!} b^{\dagger n} c^{\dagger n}\,|00\rangle$, where $T_g = \tanh(g)$, g being the squeezing parameter. To obtain ρ_h, we have to calculate $\mathrm{tr}_c\left(|\psi\rangle\langle\psi|\left(\mathbb{1} - (1-\eta_h)^{c^\dagger c}\right)\right)$. η_h stands for the efficiency of the heralding detector and tr_c is the trace on c. This can be expressed as the difference of two terms. The first one is simply the trace over $|\psi\rangle$ while the second one can be written as $\mathrm{tr}_c\left(R_h^{c^\dagger c}\,|\psi\rangle\langle\psi|\,R_h^{c^\dagger c}\right)$, with $R_h = \sqrt{1-\eta_h}$. Using the formula $R_h^{c^\dagger c} e^{T_g a^\dagger c^\dagger} = e^{R_h T_g a^\dagger c^\dagger} R_h^{c^\dagger c}$ [26], and re-normalizing the obtained state, the resulting density matrix ρ_h can be written as

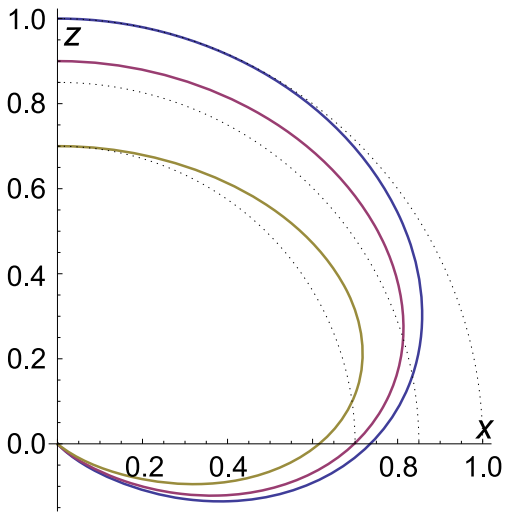

Figure 2. Focusing on the projective part μ $\{\Pi_{\vec{n}}, \Pi_{-\vec{n}}\}$ of the studied POVM, we here represent the length μ and the direction of the corresponding vector in the Bloch sphere. As we consider real α, this vector lies in the x–z plane. For unit detection efficiency ($\eta = 1$, outermost curve) and $\alpha = 0$, this vector has a unit length and is directed to the z direction. When α increases (α spans the interval $[0, 4]$), the vector starts to rotate (the polar angle gives the azimuthal angle of $\vec{n}$ on the Bloch sphere) and its length decreases (the radius decreases). In the limit of large α, the vector length tends to zero. The two inner curves corresponds to non-unit efficiency ($\eta = 90\%$ and $\eta = 70\%$, respectively).

$$\rho_h = \frac{1 - R_h^2\, T_g^2}{T_g^2\left(1 - R_h^2\right)}\left[\rho_{\rm th}\left(\bar{n} = \frac{T_g^2}{1 - T_g^2}\right) - \frac{1 - T_g^2}{1 - R_h^2 T_g^2}\rho_{\rm th}\left(\bar{n} = \frac{R_h^2 T_g^2}{1 - R_h^2 T_g^2}\right)\right], \tag{5}$$

i.e. a difference between two thermal states $\rho_{\rm th}(\bar{n}) = \frac{1}{1+\bar{n}}\sum_k \left(\frac{\bar{n}}{1+\bar{n}}\right)^k |k\rangle\langle k|$, where $\bar{n}$ is the mean photon number. Let us first calculate the correlators that would be obtained from a thermal state. We recall that a thermal state is classical with respect to the P representation. Therefore, it can be written as a mixture of coherent states $|\gamma\rangle$. Concretely, $\rho_{\rm th}\left(\bar{n}\right) = \int {\rm d}^2\gamma P^{\bar{n}}(\gamma)|\gamma\rangle\langle\gamma|$ with $P^{\bar{n}}(\gamma) = \frac{1}{\pi\bar{n}}{\rm e}^{-\frac{|\gamma|^2}{\bar{n}}}$. The correlators associated to a thermal state can thus be obtained by looking at the behavior of a coherent state. A beam splitter splits a coherent state into two coherent states, i.e. $|\gamma\rangle \rightarrow |\sqrt{R}\gamma\rangle_a|\sqrt{T}\gamma\rangle_b$, where T and R are, respectively, the transmittivity and the reflectivity. A displacement $D(\alpha)$ on a coherent state $|\gamma\rangle$ gives another coherent state with mean photon number $|\gamma + \alpha|^2$, i.e. $D(\alpha)|\gamma\rangle = |\gamma + \alpha\rangle$. From

$$(1 - \eta)^{\frac{a^\dagger a}{2}}\,|\bar{\gamma}\rangle = {\rm e}^{-\frac{\eta|\gamma|^2}{2}}\left|\sqrt{1-\eta}\,\bar{\gamma}\right\rangle, \tag{6}$$

we easily obtain the probability to get no click in both sides from a thermal state $\rho_{\rm th}(\bar{n})$ knowing the amplitudes of the local displacements α and β

$$p_{\alpha,\beta}^{\rm nc,nc} = \frac{{\rm e}^{-\eta\left(|\alpha|^2+|\beta|^2\right)+\frac{\bar{n}\eta^2}{1+\bar{n}\eta}|\sqrt{R}\alpha+\sqrt{T}\beta|^2}}{1 + \eta\bar{n}}. \tag{7}$$

Attributing the value $+1$ (-1) to a 'no-click' event ('click' event), we then obtain an explicit expression for the correlator $E_{\alpha,\beta}^{\rm th} = p_{\alpha,\beta}^{\rm nc,nc} + p_{\alpha,\beta}^{\rm c,c} - p_{\alpha,\beta}^{\rm nc,c} - p_{\alpha,\beta}^{\rm c,nc}$ associated to a thermal state $\rho_{\rm th}(\bar{n})$

$$E_{\alpha,\beta}^{\rm th} = 1 + 4\frac{{\rm e}^{-\eta\left(|\alpha|^2+|\beta|^2\right)+\frac{\bar{n}\eta^2}{1+\bar{n}\eta}|\sqrt{R}\alpha+\sqrt{T}\beta|^2}}{1 + \eta\bar{n}} - 2\frac{{\rm e}^{-\frac{\eta|\alpha|^2}{1+\eta\bar{n}R}}}{1 + \eta\bar{n}R} - 2\frac{{\rm e}^{-\frac{\eta|\beta|^2}{1+\eta\bar{n}T}}}{1 + \eta\bar{n}T}.$$

From this last expression, we deduce the correlator $E_{\alpha_i\beta_j}$ for the state (5)

$$E_{\alpha_i\beta_j} = \frac{1 - R_h^2\, T_g^2}{T_g^2\left(1 - R_h^2\right)}\left[E_{\alpha_i\beta_j}^{\rm th}\left(\bar{n} = \frac{T_g^2}{1 - T_g^2}\right) - \frac{1 - T_g^2}{1 - R_h^2 T_g^2}E_{\alpha_i\beta_j}^{\rm th}\left(\bar{n} = \frac{R_h^2 T_g^2}{1 - R_h^2 T_g^2}\right)\right]. \tag{8}$$

This explicit expression of $E_{\alpha_i\beta_j}$ allows one to optimize the CHSH–Bell value, i.e. the value of $S = |E_{\alpha_1\beta_1} + E_{\alpha_1\beta_2} + E_{\alpha_2\beta_1} - E_{\alpha_2\beta_2}|$, for given efficiencies (η, η_h) over the tunable parameters of the system, i.e. the squeezing parameter g, the amplitude of the local displacements α_i and β_j (measurement settings), and the transmittivity T of the beam splitter. Note that the CH [31] and CHSH inequalities are equivalent for all

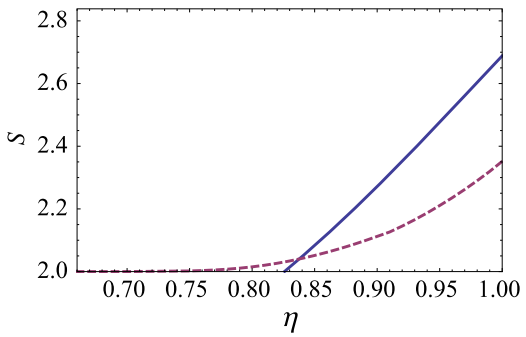

Figure 3. Optimal CHSH value as a function of the efficiency η. The full (dashed) curve is obtained in the case of spatial entanglement, see figure 1(B) (polarization-entanglement, see figure 1(A)) (see the text for detail).

probability distributions satisfying the no-signaling condition, i.e. for all quantum correlations [6]. Namely, they are related by the affine relation $4CH = S - 2$.

4. Optimization of the CHSH value

In this section, we present the result of the optimization of the CHSH–Bell value in the case of spatial entanglement (figure 1(B)). Figure 3 shows S as a function of the efficiency η and compares it to the case of polarization entanglement for which the optimization of the CHSH–Bell value has been reported in [16]. We emphasize that η is the overall detection efficiency including the transmission efficiency from the source to the detector. We assume that the efficiencies for modes a and b are the same. They are equal to the heralding efficiency $\eta_h = \eta$. Three results deserve to be highlighted.

(i) In the ideal case where $\eta = 1$, the maximal violation is around 2.69. This value is obtained in the limit $g \to 0$, i.e. when the production of multiple photon pairs is negligible. Since the heralding signal eliminates the vacuum component, we end up with a single photon Fock state in b to a very good approximation. We thus retrieve the maximal violation that can be obtained in the scenario presented in figure 1(B) with a single photon [20, 21]. Note that in practice, the value of g is limited by the probability $p_{\rm dc}$ of having a dark count in the heralding detector which is negligible if $p_{\rm dc} \ll \eta T_g^2$ only. More concretely, if one assumes that the probability of having a dark count is $p_{\rm dc} \approx 10^{-5}$ for example, we found the optimal violation $S \sim 2.67$ which is obtained for $g \sim 0.07$ and still $\eta = 1$.

(ii) We observe that the optimal state is always obtained from a 50–50 beam splitter ($R = T = \frac{1}{2}$) in the limit $g \to 0$, i.e. it is a two-qubit maximally entangled state. This is unexpected as in the case of a two-qubit state entangled in polarization, lower efficiencies can be tolerated from non-maximally entangled states [27].

(iii) The minimal required detection efficiency is $\eta_{\rm min} = 0.826$. This is counterintuitive, at least at first sight, since there is a local model reproducing the correlation of the singlet state as soon as the detection efficiency is lower or equal to $\frac{2}{\sqrt{2}+1} \approx 0.828$ [28–30]. Nevertheless, this model assumes that the probability of having a conclusive event is η whereas the probability for having a non-conclusive event is $1 - \eta$. This does not hold in the case of spatial entanglement. Let us also recall that in the scenario of spatial entanglement, the effective efficiency of the overall measurement device can be higher than the detection efficiency of the NPNR detector.

Note that the CHSH–Bell values given in figure 3 are optimized over the local strategies that are used to assign binary results ± 1 to physical events (click and no-click). We found that they are all equivalent, i.e. they all lead to the same value of S. The sum $E_{\alpha_1\beta_1} + E_{\alpha_1\beta_2} + E_{\alpha_2\beta_1} - E_{\alpha_2\beta_2}$ simply needs to be minimized or maximized depending on the strategy.

5. Rate of random bit generation

In this section, we estimate the amount of randomness created in both setups that are presented in figure 1. We present two quantities, (i) the randomness per run, i.e. the min entropy $H_{\rm min}(S)$, and (ii) the rate of randomness generation. Let us first focus on the min entropy $H_{\rm min}(S)$. As mentioned earlier in the introduction, the min-

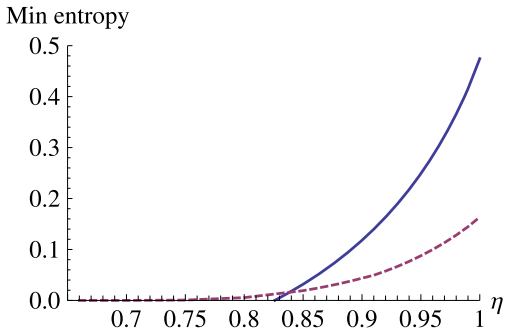

Figure 4. Min entropy per experimental run as a function of the efficiency η. The full (dashed) curve corresponds to the case of spatial entanglement (figure 1(B)) (polarization-entanglement, see figure 1(A)).

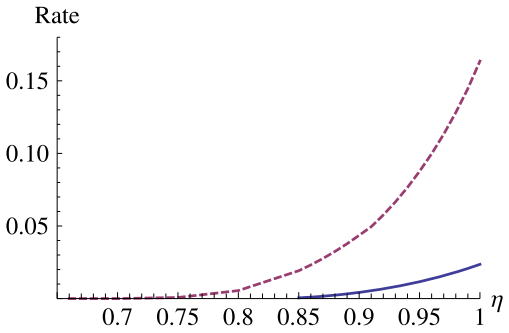

Figure 5. Rates of random bits (in unit of the pump-laser rate) as a function of the efficiency η. The full (dashed) curve corresponds to the case of spatial-entanglement (polarization-entanglement).

entropy rate (amount of randomness per bit) can be lower bounded in terms of the observed CHSH violation S [4]. The lower bound is given by

$$H_{\min}(S) = 1 - \log_2\left(1 + \sqrt{2 - \frac{S^2}{4}}\right). \tag{9}$$

$H_{\min}(S)$ is equal to 0 when S is 2 and it reaches its maximum value 1 when S is maximal, i.e. $S = 2\sqrt{2}$.[6] Since the min entropy is a monotonic function of S, large S favors large min entropy. The optimal value of $H_{\min}(S)$ computed from [4] for the two different implementations of figure 1 is shown in figure 4. Since a larger violation can be obtained in the scenario involving spatial entanglement, the scheme of figure 1(B) provides higher min entropy than the scheme of figure 1(A) for large enough efficiencies. On the other hand, the scenario involving the spatial-entanglement requires efficiencies higher than 0.826 while the scenario with polarization-entangled states allows one to get small but non-zero min entropy for efficiencies in between ≈0.67 and 0.826.

Let us now focus on the rate of randomness generation. It is given by

$$R(S) = rH_{\min}(S), \tag{10}$$

where r is the rate at which the states are analyzed. Consider first the case where the repetition rate is set by the pump laser. For the conventional setup (figure 1(A)) $R(S) = r_{\text{pump}} H_{\min}(S)$ whereas in the case of spatial entanglement, the rate at which the states are analyzed is intrinsically limited by the heralding rate, i.e. $R(S) = r_{\text{pump}} \frac{\eta_h T_g^2}{1-(1-\eta_h)T_g^2} H_{\min}(S)$. Assuming $\eta_h = \eta$, we have optimized $R(S)$ over the squeezing parameter g, the values of α_i and β_j, and the transmittivity T. The result is shown in figure 5 and is compared to the conventional scenario (see figure 1(A)). One sees that the high violations that are obtained in the scenario involving the spatial entanglement do not compensate the reduction of the repetition rate.

Consider now the situation where the rate is not limited by the pump laser but by the speed at which the measurement settings are chosen, as in [10], or by the deadtime of the detectors so that the heralding rate (r_{d}) in

[6] Note that higher bounds can *a priori* be obtained by considering the outcomes observed by two parties, or by evaluating the min entropy based on all observed statistics (rather than just the value of CHSH), see [32].

the scenario given in figure 1(A) is the same that the detection rate of the scenario of figure 1(B). In this case, the rate of random bits is given by $R(S) = r_d H(S)$ and can thus be deduced from figure 4. It is clear that the rate of randomness in the scenario involving spatial entanglement is substantially higher than the conventional one (figure 1(A)) for efficiencies larger than 0.84 as its Bell violation is higher. Furthermore, in practice, randomness extraction is normally carried out on a fixed input bit string and the size of the output string is approximately given by the min-entropy of the input bit string. Seen from this point of view, it is clear that our spatial entanglement setup allows a larger number of extractable secret bits for a fixed input bit string.

6. Conclusion and discussions

Motivated by very recent experiments reporting on the first-detection-loophole-free Bell tests with photon pairs, we have studied two different scenarios, both of them based on SPDC sources and photon counting techniques, for the generation of random bits. In particular, we have shown how to calculate the correlators in the scenario involving spatial entanglement (represented in figure 1(B)) in a non-perturbative way. This allowed us to optimize the CHSH–Bell value, that we have compared to the one obtained in the more conventional scenario of figure 1(A). While the detection technique of the scenario given in figure 1(B) involves small displacement operations, i.e. requires a noise free local oscillator indistinguishable from the photons to be detected, and overall detection efficiencies larger than in the conventional scenario, the scenario involving spatial entanglement has several interesting features:

(i) First, only one mode needs to be detected efficiently. Therefore one can use filtering techniques on the heralding mode to prepare it in a mode having high coupling and detection efficiency [33, 34].

(ii) For efficiencies higher than 84%, the scenario based on spatial entanglement leads to substantial improvements over the conventional setup in terms of min entropy.

(iii) Assuming that the number of experimental runs is large enough so that the Bell violation is accurately estimated in both setups, we have shown that in the realistic regime where the repetition rate is limited e.g. by the detector dead time in both scenarios, the higher CHSH–Bell violation of the scenario with spatial entanglement leads to higher bit rates than the one of the conventional scenario.

We believe that these advantages could provide motivations for several experimental research groups to realize detection-loophole free Bell tests following the idea that Banaszek and Wodkiewicz [18] have initiated more than 15 years ago.

Acknowledgments

We thank V Scarani, T Barnea, and G Pütz for discussions and comments. This work was supported by the Swiss NCCR QSIT, the Swiss National Science Foundation SNSF (grant PP00P2 – 150579 and 'Early PostDoc. Mobility'), the European Commission (IP SIQS, Chist-era DIQIP), the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and the Singapore National Research Foundation.

References

[1] Jennewein T, Achleitner U, Weihs G, Weinfurter H and Zeilinger A 2000 *Rev. Sci. Instrum.* **71** 1675–80
[2] Stefanov A, Gisin N, Guinnard O, Guinnard L and Zbinden H 2000 *J. Mod. Opt.* **47** 4
[3] Dynes J F, Yuan Z L, Sharpe A W and Shields A J 2008 *Appl. Phys. Lett.* **93** 031109
[4] Pironio S *et al* 2010 *Nature* **464** 1021
[5] Colbeck R and Kent A 2011 *J. Phys. A: Math. Theor.* **44** 095305
[6] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 *Rev. Mod. Phys.* **86** 839
[7] Rowe M A, Kielpinski D, Meyer V, Sackett C A, Itano W M, Monroe C and Wineland D J 2001 *Nature* **409** 791
[8] Matsukevich D N, Maunz P, Moehring D L, Olmschenk S and Monroe C 2008 *Phys. Rev. Lett.* **100** 150404
[9] Hofmann J, Krug M, Ortegel N, Gérard L, Weber M, Rosenfeld W and Weinfurter H 2012 *Science* **337** 72
[10] Christensen B G *et al* 2013 *Phys. Rev. Lett.* **111** 130406
[11] Giustina M *et al* 2013 *Nature* **497** 227
[12] Lita A E, Miller A J and Nam S W 2008 *Opt. Express* **16** 3032
[13] Miller A J, Lita A E, Calkins B, Vayshenker I, Gruber S M and Nam S W 2011 *Opt. Express* **19** 9102–10
[14] Fukuda D *et al* 2011 *Opt. Express* **19** 870–5
[15] Verma V B, Korzh B, Bussières F, Horansky R D, Lita A E, Marsili F, Shaw M D, Zbinden H, Mirin R P and Nam S W 2014 *Appl. Phys. Lett.* **105** 122601

[16] 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
[17] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880
[18] Banaszek K and Wodkiewicz K 1998 *Phys. Rev. Lett.* **82** 2009
[19] Tan S M, Walls D F and Collett M J 1991 *Phys. Rev. Lett.* **66** 252
[20] Chaves R and Brask J Bohr 2011 *Phys. Rev.* A **84** 062110
[21] Bohr Brask J, Chaves R and Brunner N 2013 *Phys. Rev.* A **88** 012111
[22] Torlai G, McKeown G, Marek P, Filip R, Jeong H, Paternostro M and De Chiara G 2013 *Phys. Rev.* A **87** 052112
[23] Seshadreesan K P, Wildfeuer C, Kim M B, Lee H and Dowling J P 2013 arXiv:1310.1410
[24] Hessmo B, Usachev P, Heydari H and Björk G 2004 *Phys. Rev. Lett.* **92** 180401
[25] D'Ariano G M, Lo Presti P and Perinotti P 2005 *J. Phys. A: Math. Gen.* **38** 5979–91
[26] Sekatski P, Sanguinetti B, Pomarico E, Gisin N and Simon C 2010 *Phys. Rev.* A **82** 053814
[27] Eberhard P H 1993 *Phys. Rev.* A **47** R747
[28] Garg A and Mermin N D 1987 *Phys. Rev.* D **35** 3831
[29] Larsson J-Å 1998 *Phys. Rev.* A **57** R3145
[30] Massar S and Pironio S 2003 *Phys. Rev.* A **68** 062109
[31] Clauser J and Horne M 1974 *Phys. Rev.* D **10** 526535
[32] Nieto-Silleras O, Pironio S and Silman J 2014 *New J. Phys.* **16** 013035
Bancal J-D, Sheridan L and Scarani V 2014 *New J. Phys.* **16** 033011
[33] Pomarico E, Sanguinetti B, Guerreiro T, Thew R and Zbinden H 2012 *Opt. Express* **20** 23846
[34] Guerreiro T, Martin A, Sanguinetti B, Bruno N, Zbinden H and Thew R T 2013 *Opt. Express* **21** 27641