Certified Randomness from Bell’s Theorem and Remote State Preparation Dimension Witness

Xing Chen,1 Kai Redeker,2 Robert Garthoff,2 Wenjiamon Rosenfeld,2 Jörg Wrachtrup,1,3 and Ilja Gerhardt1

1,3. Institute of Physics, University of Stuttgart and Institute for Quantum Science and Technology (IQST), Pfaffenwaldring 57, D-70569 Stuttgart, Germany
2Fakultät für Physik, Ludwig-Maximilians-Universität München, D-80799 München, Germany
3Max Planck Institute for Solid State Research, Heisenbergstraße 1, D-70569 Stuttgart, Germany

Randomness can be device-independently certified from a set of experimental data by Bell’s theorem without placing assumptions about the experimental devices. The certification procedure in previous studies underestimated the generated randomness, due to a non-optimal lower bound of the entropy. We solve this by developing an analytic upper bound for the joint outcome probability \( p(ab|xy) \), and show that the lower the Bell inequality violation value is, the more advantageous the use of the joint outcome probability becomes. In the same experimental data, when a few general assumptions are introduced to characterize the experimental setups, substantially more semi-device-independent randomness can be certified by a witness we call remote state preparation dimension witness without using Bell’s theorem. This is one important step towards practical use.

Random numbers have a wide variety of applications in daily life [1]. Their use covers gambling, scientific research [2], and most importantly, cryptography [3]. Naturally, a given bit string can not be proven to be random [1], and the generation process of a random number is the relevant measure. Quantum-mechanical processes are believed to be the only known source of randomness in nature, thus the generation of a random bit by a quantum mechanical superposition is desirable [4]. Many quantum mechanical measurements show a probabilistic outcome [5], however, this can have other, technical causes [6, 7], than quantum mechanics.

Therefore, to generate a reliable quantum random number, i.e. one which directly stems from a quantum process and is free from other noise sources or manipulation, we need to utilize a process which proves its “quantumness” in the course of a measurement. The usage of fundamental physics inequalities can realize this goal. From Bell inequalities [8], for example, the Clauser-Horne-Shimony-Holt (CHSH) inequality [9], random numbers can be certified in a device-independent (DI) way [6, 10–13]. Device-independence means, that we do not need technical insights into the generation process, but that the violation can be derived in an abstract fashion. Certification means in this context, that a quantifiable physical measure exists, which guarantees that the randomness arises from a quantum process.

Although Bell’s theorem seems to be the ideal way to certify quantum randomness, this method remains experimentally challenging [14–17] and has low randomness output rate [10, 12]. Therefore, other semi-device-independent randomness certification methods have been developed. Semi-device-independent means that the raw measurement outcomes reveal their quantumness, if a certain number of assumptions of the experimental setup can be guaranteed [18]. The Kochen-Specker inequality [19] and the dimension witness [20] certify the generated random numbers in a semi-device-independent (SDI) way [21–23].

![Bell Test Diagram](image)

FIG. 1: A Bell test involves two physically separated systems, and two given input bits \( x, y \) generates (partially correlated) outcomes \( a, b \). The Bell correlation value \( S \), allows in a DI scenario to quantify the amount of randomness; another scenario is to extract SDI randomness, when remote state preparation (RSP) dimension witness is utilized.

Here, we certify and extract the randomness generated in a loophole-free Bell test [17], in a DI and a SDI manner. For the DI approach we utilize an analytical bound of the randomness that improves the analytical result from [10]. The new bound which yields more randomness per output is especially advantageous in the case of a small violation of the CHSH inequality. For the SDI approach, which needs additional assumptions on the devices, we introduce a remote state preparation dimension witness, which allows for a significantly higher output rate of random bits.

**CHSH scenario**—For the CHSH inequality [9], an experiment with pairs of particles and two parties, Alice and Bob, is considered. In each round of the experiment, each party receive one particle of a pair and perform a local measurement on it, using one out of two measurement settings. The choice of the local measurement settings depends on the randomly chosen binary input \( x \) for Alice and \( y \) for Bob. The measurements produce a binary output \( a \) for Alice and \( b \) for Bob (Fig. (1)).

The correlation value \( S \) of the CHSH inequality is \( S = \sum_{x,y} (-1)^{xy} [P(a = b|xy) - P(a \neq b|xy)] \) [24], where \(| . |\) denotes the absolute value, and \( P(a = b|xy) \) (or \( P(a \neq b|xy) \))

...
b(x,y)) is the probability that output \( a = b \) (or \( a \neq b \)) when the measurement settings \((x, y)\) are chosen. For all local realistic theories \( S \) cannot exceed the maximum value of 2. In contrast, quantum mechanics allows the value of \( S \) to be between 2 and \( 2\sqrt{2} \) [8, 25].

The aforementioned experiment is performed as a loophole-free Bell test in \[17\]. In this Bell test, Alice and Bob each operate an atom trap for a single rubidium atom. The traps, separated by 398 m, are independently operated, comprising an own laser system and control electronics. The atomic qubits are encoded in the \( m_F = \pm 1 \) Zeeman sub-level of the 5\( S_{1/2} \), \( F = 1 \) ground state, with \( \mid \uparrow \rangle_z \) corresponding to \( m_F = +1 \), \( \mid \downarrow \rangle_z \) corresponding to \( m_F = -1 \). To generate entanglement between Alice and Bob’s remote atoms, an atom-photon entanglement and a subsequent Bell state measurement (BSM) on the two emitted photons was used \[26, 27\].

For the creation of the entangled atom-photon pairs, each atom is excited to the 5\( S_{1/2} \) Zeeman sub-level of the 5\( S_{1/2} \), \( F = 1 \) ground state via a short laser pulse. The subsequent spontaneous emission yields to a photon whose polarization is entangled with the atomic qubit state. Both photons are coupled into single mode fibers and are guided to the BSM setup, where two photon interference on a fiber beam splitter together with photon polarization analysis is employed to project the photons on two out of the four possible Bell states. The photonic measurement heralds the creation of one of the entangled atom before ionization. For the choice of the setting each party employs a QRNGs outputting freshly generated random bits on demand. The total time needed from the generation of the input \( x \) or \( y \) to receiving the output \( a \) or \( b \) is less than 1.1 \( \mu \)s, together with a separation of the atom traps of 398 m this enables for space-like separation of the measurements \[28\]. Thus, the experiment enforced the assumptions made for deriving the CHSH inequality. In total, 55568 rounds were recorded, 27885 with the \( \mid \Psi^+ \rangle \) prepared and 27683 with the \( \mid \Psi^- \rangle \).

**DI certification protocol**—As outlined above, device independence can be linked to the violation of Bell inequality \[29\]. This means, as long as Bell inequality is guaranteed to be violated, true randomness can be generated. Although the randomness certified by Bell’s theorem can be device independent, we still need some extra assumptions to bound the randomness in this model \[10\]: (1) the remote parties perform local and independent measurements on their ideally space-like separated (=perfectly shielded) devices; (2) the measurement settings \((x, y)\) are not determined beforehand and are unpredictably chosen; (3) the measurement process is described by quantum mechanics, and nature is not e.g. pre-determined as a whole. In a loophole-free Bell test the assumption (1), which is required for a loop-hole free Bell test is fulfilled. Assumption (2) means that the \( i-th \) input \( x_i \) and \( y_i \) are not known to the experimental devices until the \( i-th \) run of the experiment.

In \[10\], the marginal guessing probability \( p(a|x) \) had been connected to the correlation value \( S \) of the CHSH inequality. This allows to bound the randomness to 1 bit per event when \( S = 2\sqrt{2} \). However, for \( S = 2\sqrt{2} \), the randomness per event from a CHSH experiment is as high as 1.23 \[30–32\]. Obviously, the marginal guessing probability does not give us a tight lower bound of the DI randomness. Previously, the bound of 1.23 bits/event was derived by semi-definite-programming \[10\]. Unfortunately, this method relies heavily on computational power. To bound the full amount of randomness of the data set, we introduce an analytic min-entropy bound from the joint outcome probability \( p(ab|xy) \). Accordingly, when the correlation value of the CHSH inequality reaches \( 2\sqrt{2} \), the bound 1.23 bits per event is reached.

The randomness per event is quantified by the conditional min-entropy \( H_\infty(AB|XY) \) (where \( A, B, X, Y \) represent the set of random variables \( a, b, x, y \)). It is defined as \( H_\infty(AB|XY) = -\log \max_{abxy} p(ab|xy) \). When considering the relationship between Alice and Bob’s measurement settings and the correlation value \( S \), \( \max_{abxy} p(ab|xy) \) is derived as

\[
\max_{abxy} p(ab|xy) \leq \frac{1}{2} \left( 1 + \sqrt{2 - \frac{S^2}{4}} \right) \left( \frac{1}{2} + \frac{1}{S} \right).
\]

This upper bound of \( \max_{abxy} p(ab|xy) \) is derived from the worst case scenario, and it is the maximum guessing probability for a given \( S \) value. See the supplementary for details.

In comparison to the prior analytical bound on the randomness \[10\], the new bound allows for a significantly higher guaranteed randomness per event. The improvement is at least a factor of 1.23, in case of \( S = 2\sqrt{2} \), and increases to a factor of nearly 2 for \( S \) close to 2, see Figure 2.

**SDI certification protocol**—For the certification of the randomness from a Bell test, Bell inequalities must be violated. Unfortunately, the loophole free Bell experiments \[14–17\], while showing a significant violation of the classical bound, did not reach the maximally allowed values for quantum mechanics. Thus only a small amount of randomness per round can be certified in the DI manner. In the worst case, no randomness can be certified \[33\]. This means only a few random bits can be extracted from many experimental rounds. However, when we introduce additional assumptions and leave the DI scenario, this situation is changed. In order to build the experimental devices, it is necessary to have some knowledge about
the way they function e.g. the devices are error prone but not maliciously built. This knowledge allows for a higher bound of the randomness per event for the same experiment. Using a dimension witness is one possible way for such a higher bound of the randomness.

The idea of dimension witness was first introduced in [34]. After this pioneering paper, a substantial number of studies have been performed on this concept [20, 31, 35–37].

Before applying the dimension witness to the Bell experiment with entangled atoms, we first show that the experiment admits a 2-dimensional quantum representation.

In our Bell test, there are two inputs $x, y$ and two outputs $a, b$. When Alice does one of her two measurements, the entangled state of Bob’s side will randomly collapse into one specific state. Since Alice has two different measurement settings and each measurement setting has two different measurement results, when she does her two measurements randomly multiple times, Bob’s side will get four quantum states. These four quantum states in Bob’s side are represented as $x'$, and $p(b|x', y) = p(ab|xy)/p(a|x, y)$.

Notice that, $p(ab|xy) = p(a|xy)p(b|x, a, y)$, therefore $p(b|x', y) = p(b|x, a, y)$. So we can treat Alice’s outputs as the input parameter [31], this means that Alice’s input $x$ and result $a$ together can be treated as the state labels $x'$ for Bob. Furthermore, $p(b|x', y)$ can be re-written as (see supplementary)

$$p(b|x', y) = \frac{p(ab|xy)}{p(a|x, y)} = \text{Tr} \left( \rho_{a|x} M^B_{b | y} \right),$$

where $\rho_{a|x}$ is the state on Bob’s side when Alice performs her measurement $x$ and gets a result $a$. $M^B_{b | y}$ is the measurement operators in Bob’s side. $\rho_{a|x}$ and $M^B_{b | y}$ are acting on $\mathbb{C}^2$ (a 2-dimensional complex coordinate space). Subsequently, $p(b|x', y)$ admits a 2-dimensional quantum representation [20, 34, 35]. This shows that we can use the dimension witness to quantify the quantumness in our experiment.

Different kinds of dimension witnesses can be used in a 2-dimensional quantum representation. The dimension witness we used here is was introduced in [20]. The advantage of this dimension witness is that it can be used for arbitrary dimensionality and accounts for technical imperfections. Most importantly, it can be used to certify randomness [20]. It is defined as

$$W = \frac{p(1|0, 0) - p(1|1, 0)}{p(1|0, 0)} - \frac{p(1|2, 0) - p(1|3, 0)}{p(1|0, 0)},$$

where $p(b|x', y)$ is defined in Eqn. (2), and the result $b$ is chosen as “1” in the above definition. The definition equation of the dimension witness here is the same as in [20], but the state $x'$ differs. In our case, the state $x'$ is in Bob’s side, but its preparation is completed by the projective measurement of Alice, so the state $x'$ is remotely prepared [38, 39]. In order to emphasize this difference, we name it as remote state preparation (RSP) dimension witness. The remote state preparation needs to be ensured either by placing the devices each in its own perfectly shielded laboratory or as it is done our loophole-free Bell test [17] with space-like separation of the measurements in each device.

From the above definition, the RSP-dimension witness $W_B$ for Bob’s side is constructed. Similarly, $W_A$ can be constructed for Alice’s side. We define $W_{\text{rsp}} = \min\{W_A, W_B\}$, and use $W_{\text{rsp}}$ as the RSP-dimension witness in the following model. The RSP-dimension witness captures the quantumness of the preparation and measurements in our Bell test. If the preparations are classical, one has $W_{\text{rsp}} = 0$, while a quantum preparation and measurement leads to $0 < W_{\text{rsp}} \leq 1$.

Although, $S$ and $W_{\text{rsp}}$ are based on the same experimental data, they are not directly linked. Generally speaking, $S$ cannot be used to calculate the value of $W_{\text{rsp}}$, it only affects the lower limit of $W_{\text{rsp}}$. For example, when $S = 2$, $W_{\text{rsp}} \in [0, 1]$, and when $S = 2\sqrt{2}$, $W_{\text{rsp}} = 1$.

Before using the RSP-dimension witness to bound the randomness generated during the experiment, we discuss the required assumptions. As before, we require, that the above (DI) assumptions (1, 2, 3) hold true. Besides, there are some extra assumptions [23]: (4) the dimensionality of the quantum system is fixed during the experiment; (5) the system is memoryless and subsequent outcomes are not directly correlated. As before, we require that the remote devices are independent and are not classically correlated (assumption (1)). This implies that the experimental devices do not have any pre-established correlations among each other; this also indicates that the devices that are used to generate the input strings $x, y$ are not correlated with the measurement devices. Subsequently, $x, y$ can be pseudo-random numbers, as long as they are independent, i.e. not correlated, from each other.
and the measurement apparatus. Assumption (4) means that the entropy contains in the measurement result of measuring $x'$ does not exceed 1 bit, a possible violation would be that the information about $x'$ is duplicated by or correlated with extra qubits.

The assumption (4) can be relaxed by the space-like separation of Alice and Bob in our Bell test. In general, a bipartite entangled state shared between Alice and Bob has two different measurement results in each side with one measurement setting—it can be described by a qubit. As for the given experiment, the state preparation of the RSP-dimension witness is independently completed by two sides: one side performs the measurement and the other side gets the state simultaneously. Under space-like separation, when the state is prepared by one side, the measurement is performed outside the light cone of state preparation. Thus, it is impossible for the state preparation devices to send extra qubits of the prepared states to the measurement devices without lowering the values of $W_{\text{rsp}}$ [40]. As long as $W_{\text{rsp}} > 0$, the remote measurements are exceeding a classical correlation.

Since the inputs $x$ and $y$ are independent from each other, and in the experiment, different choices of the measurement settings are uniformly random, thus each combination of $x$ and $y$ occurs with probability $1/4$ [23]. Then, the guessing probability $p_{\text{guess}}$ of $p(ab|xy)$ is

$$p_{\text{guess}}(ab|xy) = \frac{1}{4} \sum_{x,y} \max_{a,b} p(ab|xy).$$

The right part of the equation satisfies

$$\frac{1}{4} \sum_{x,y} \max_{a,b} p(ab|xy) \leq \max_{x,a} \frac{1}{2} \sum_{y} \max_{a,b} p(b|(x,a), y).$$

From basic mathematical calculations, the inequalities in Eqn. (5) can be deduced (see supplementary). The upper bound of $\frac{1}{2} \sum_{x,a} \max_{b} p(b|(x,a), y)$ is shown in [23]. The upper limit of $\max_{x,a} p(a|x)$ with the given $W_{\text{rsp}}$ is derived in the supplementary. Putting the above results together, the upper limit of $p_{\text{guess}}(ab|xy)$ is

$$\leq \left(1 + \sqrt{1 - W_{\text{rsp}}^2} \right) \frac{1}{2} \left(1 + \sqrt{1 - W_{\text{rsp}}^2} \right).$$

As we can see, the equation of guessing probability $p_{\text{guess}}(ab|xy)$ from $W_{\text{rsp}}$ is not the same as the one from [23]. The difference is caused by $\max_{x,a} p(a|x)$, which represents the quantum measurement from the state preparation process.

The conditional min-entropy $H_\infty(AB|XY)$ in this situation is $H_\infty(AB|XY) = -\log_2 p_{\text{guess}}(ab|xy)$. This equation allows us to bound the randomness in the experimental data in a SDI way. The randomness per event from the RSP-dimension witness model is depicted in Fig. (3). Compared to [23], the introduction of quantum measurements in the state preparation process gives us a significant advantage to bound the randomness in our experimental data. For instance, the maximum certified randomness in our model is 1.23 bits per event [41], which is significantly larger than the previous dimension witness model [23].

![FIG. 3: Output randomness utilizing the dimension witness. The nonzero RSP-dimension witness $W_{\text{rsp}}$ gives us a new perspective to bound the randomness in the experimental data. The blue curve displays the randomness certified by the $W_{\text{rsp}}$, while the dashed purple curve represents the randomness certified by the previously defined dimension witness [20]. Clearly, the combination of remote state preparation and the dimension witness increase the bound of randomness per event, as compared to a normal dimension witness certification model in [23].](image-url)
which are much less complex than the loophole-free Bell test \[17\]. As shown, since the first model has higher bound than the earlier model \[10\], more DI randomness can be extracted in the experimental events. The second model improves the bound of the randomness from the data tremendously. Of course, the second model offers weaker security guarantees for randomness than the first model, but it is still certified randomness under SDI conditions. Also, the requirements in the SDI model can be fulfilled by standard technologies, which are much less complex than the loophole-free Bell test.

Next we apply our two methods to bound the randomness produced in the Bell test with entangled atoms \[17\] and then extract the randomness with hashing functions. In the following randomness extraction, due to the finite data size, the confidence level of the model and the error of hashing functions are introduced. The confidence level is taken as 99\% with reference to \[10, 23\], and the error of the hashing functions is chosen as 0.001. We use universal hashing functions to extract the bounded randomness, see supplementary for details. Considering the state, the collected data resulted in \( S = 2.085 \), and with a total number of events \( n = 27885 \), only 195 bits DI randomness can be extracted for this state. We calculate the RSP-dimension witness value for this entangled state as \( W_{\text{rsp}} = 0.542 \). The SDI randomness extracted in all 27885 events amounts to 3821 bits.

Performing the same task for the 27683 events from the state, the value of \( S \) amounts to 2.177, and the RSP-dimension witness value is \( W_{\text{rsp}} = 0.591 \). The extracted DI randomness in 27683 events amounts to 2046 bits, while the SDI randomness amounts to 4660 bits.

Conclusion—We have presented two methods to bound the randomness from a Bell test. Their applicability holds especially for the CHSH-variant of the test \[25\]. The first model comprises an analytic upper bound for the joint outcome probability \( p(ab|xy) \). With this upper bound, the global DI randomness in the experimental data can be extracted. The analytic bound is more conveniently applicable than earlier semi-definite-programming methods.

An extended RSP-dimension witness model is developed for same version of Bell test \[25\]. In this model, the bound of randomness per event is significantly higher than the first model, and it is still possible to extract randomness with this model when the Bell inequality is not violated.

We have applied the two models to the data from a loophole-free Bell test \[17\]. As shown, since the first model has higher bound than the earlier model \[10\], more DI randomness can be extracted in the experimental events. The second model improves the bound of the randomness from the data tremendously. Of course, the second model offers weaker security guarantees for randomness than the first model, but it is still certified randomness under SDI conditions. Also, the requirements in the SDI model can be fulfilled by standard technologies, which are much less complex than the loophole-free Bell test.
10.1103/PhysRevLett.119.010402.

[18] For the semi-device-independent protocols mentioned in this letter, the assumptions about the experimental devices should be general, which means they are not supposed to characterize the devices in details, and they do not belong to source-independent or measurement-device-independent protocols.

[19] S. Kochen and E. P. Specker, Journal of Mathematics and Mechanics 17, 59 (1967), ISSN 00959057, 19435274, URL http://www.jstor.org/stable/2492153.

[20] J. Bowles, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. 112, 140407 (2014), URL https://link.aps.org/doi/10.1103/PhysRevLett.112.140407.

[21] M. Um, X. Zhang, J. Zhang, Y. Wang, Y. Shen, D.-L. Deng, L.-M. Duan, and K. Kim, Scientific Reports 3, 1627 EP (2013), article, URL https://doi.org/10.1038/srep01627.

[22] M. Jerger, Y. Reshitnyk, M. Oppliger, A. Potocnik, M. Mondal, A. Walraff, K. Goodenough, S. Wehner, K. Juliusson, N. K. Langford, et al., Nature Communications 7, 12930 (2016), ISSN 2041-1723, URL https://doi.org/10.1038/ncomms12930.

[23] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. 114, 150501 (2015), URL https://link.aps.org/doi/10.1103/PhysRevLett.114.150501.

[24] In order to allow for a violation of the CHSH inequality, for certain states and measurement settings combinations, a permutation of the values of $a$ and $b$ might be necessary.

[25] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969), URL https://link.aps.org/doi/10.1103/PhysRevLett.23.880.

[26] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. 71, 4287 (1993), URL https://link.aps.org/doi/10.1103/PhysRevLett.71.4287.

[27] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. 80, 3891 (1998), URL https://link.aps.org/doi/10.1103/PhysRevLett.80.3891.

[28] J.-Å. Larsson, Journal of Physics A: Mathematical and Theoretical 47, 424003 (2014), URL https://doi.org/10.1088/1751-8121/47/42/424003.

[29] R. Colbeck, PhD dissertation, Univ. Cambridge (2009).

[30] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. 108, 100402 (2012), URL https://link.aps.org/doi/10.1103/PhysRevLett.108.100402.

[31] H.-W. Li, P. Mironowicz, M. Pawlowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 87, 020302 (2013), URL https://link.aps.org/doi/10.1103/PhysRevA.87.020302.

[32] J.-D. Bancal, L. Sheridan, and V. Scarani, New Journal of Physics 16, 033011 (2014), URL https://doi.org/10.1088%2F1367-2630%2F16%2F3%2F033011.

[33] This maybe caused by (i) the finite amount of events or (ii) simply that Bell inequality is not violated.

[34] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. 100, 210503 (2008), URL https://link.aps.org/doi/10.1103/PhysRevLett.100.210503.

[35] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. 105, 230501 (2010), URL https://link.aps.org/doi/10.1103/PhysRevLett.105.230501.

[36] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 84, 034301 (2011), URL https://link.aps.org/doi/10.1103/PhysRevA.84.034301.

[37] M. Pawlowski and N. Brunner, Phys. Rev. A 84, 010302 (2011), URL https://link.aps.org/doi/10.1103/PhysRevA.84.010302.

[38] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, Phys. Rev. Lett. 87, 077902 (2001), URL https://link.aps.org/doi/10.1103/PhysRevLett.87.077902.

[39] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, IEEE Transactions on Information Theory 51, 56 (2005), ISSN 1557-9654.

[40] This means, the extra qubits sent out by the state preparation devices can be treated as classical noise in this situation.

[41] The maximum certified randomness per event is 1.23 bits for both DI and SDI models. This is not a coincidence, since when $S = 2\sqrt{2}$, the measurement settings of Alice and Bob are in ideal case, and the measurement results of different measurement settings has the same maximum guessing probability--0.4268, and -- $\log_2 0.4268 = 1.23$.

[42] H.-W. Li, M. Pawlowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A 85, 052308 (2012), URL https://link.aps.org/doi/10.1103/PhysRevA.85.052308.

[43] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. 68, 557 (1992), URL https://link.aps.org/doi/10.1103/PhysRevLett.68.557.