Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 14
TPCEE 2026

Advances in Device-Independent and Semi-Device-Independent Quantum Random Number Generation

Jingwei Tang *

Department of physics, University College London, London, United Kingdom

* Corresponding Author Email: zcapjt0@ucl.ac.uk

Abstract. The generation of quantum random numbers (QRNG) is of great importance in the fields of cryptography and fundamental physics. However, in real applications, there is a large trade-off between the operation efficiency and the security guarantee. Protocols that are fully DI give the best security, by using loophole-free Bell tests, but they have remarkably low generation rates. On the other hand, the schemes that assume trusted devices can go very high speed, but they rely on assumptions that cannot be checked by themselves. This review follows the path from the basic loophole free Bell tests to the functional QRNG, and the author highlights five important experiments done from 2010 to 2025. The author analyzes the theoretical proof of the randomness that one gets from the Bell inequality violations, the first concurrent closure of both detection and locality loophole, the first fully DI QRNG, and the recent chip-based source-device-independent realization that can go over 20 Gbps. These results show a clear passage from the first proof of concept demonstrations to compact integrated systems, and this paper ends up with the assessment that the semi-DI methods are a nice compromise in between.

Keywords: Quantum random number generation; Loophole-free Bell tests; randomness certification.

1. Introduction

Genuine randomness is also an essential ingredient of today s information technology. From cryptographic systems and numerical modeling to basic investigations in physics applications, everything depends essentially on the presence of truly random numbers [1]. The usual algorithmic methods give only pseudo-random sequences - these are deterministic and in principle predictable if one knows the initial seed and the generating algorithm. Quantum mechanics provides a solution to this: the indeterminacy associated to the quantum measurement processes is a true source of randomness that no deterministic procedure can mimic [2].

Quantum random number generators (QRNGs) make use of the natural unpredictability of quantum phenomena. This allows to have a high speed of the number generation, but at the same time, makes the system vulnerable for the problems due to hidden defects or known intentional tampering [1]. On the other side, in the device independent (DI) QRNGs there is not any trust in the equipment: the security of them is guaranteed only with the observation of a Bell inequality violation [3]. This is the highest possible level of a security. But the practical implementation requires very difficult experimental conditions, Bell tests without all the known loopholes, with high detection efficiency and with a spacelike separation between the measurement events [4]. Therefore, the rates at which the random numbers can be generated with this method are very limited at the moment.

A loophole-free Bell experiment is the one that requires to remove at the same time both the detection loophole, that is to detect a sufficiently large proportion of the events, and the locality loophole, that is to ensure a spacelike separation between the measurement events. It was not possible to fulfill at the same time these two requirements for more than four decades. The first big step was in 2015, when Hensen and co. have solved both the loopholes of using the so-called nitrogen-vacancy (NV) centers in a diamond separated by a distance of 1.3 kilometer [5]. Soon after, the work of Shalm et al. have done the same with entangled photons [6]. Those two studies showed that the violations of Bell inequalities would be from now on, detected without the need of some extra presumption as the fair

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

sampling hypothesis, and that were the ground to put protocols in quantum information that do not depend on the particular devices.

The work of Liu et al. then realized the transition from loophole-free Bell experiments to practical device-independent quantum random number generators (DI-QRNGs). By combining very efficient single-photon detection with the entropy accumulation principle, they have generated verified random bits at a speed of 181 bits per second [7]. More recently, the semi-device-independent (SDI) paradigm has appeared as a practical middle ground. Bertapelle et al. have implemented this with an integrated photonic source-device-independent QRNG that works at rates above 20 gigabits per second [8]. This same certification methodology, based on Bell tests, has also been used for quantum key distribution protocols [9] and for randomness expansion protocols [10], which indicates that it is wider relevant than in the domain of random number generation.

This review is devoted to the history of the very recent device-independent and semi-device-independent QRNGs. The author will follow the evolution of the devices from the first Bell test experiments to their present realization as integrated chip-scale ones. The author reviews several experimental studies and then discusses in which way they are methodologically addressed, how they close the loopholes, and the operational performance indicators they give.

2. Methods

2.1. SDP-Based Min-Entropy Certification

Pironio et al. established the theoretical knowledge base for certifying randomness from Bell violations using semidefinite programming (SDP) to compute a lower bound on the conditional min-entropy $H_{min}(R|S)$. For a known CHSH expectation I, the bound is

$$H_{min}(R|S) \geq nf\left(\hat{I} - \epsilon\right) \tag{1}$$

where is $\hat{I}$ the estimated CHSH value, ϵ represents finite-statistical fluctuations, and $f(I)$ is a convex function derived from SDP. This method does not assume independent and identically distributed (i.i.d.) behavior, thereby ensuring robustness against memory effects.

In the experiment, the author used two trapped $^{171}Yb^{+}$ ions entangled via photon-mediated swapping, with spin-state readout achieved through fluorescence detection at near-unit efficiency-thereby closing the detection loophole. However, the locality still exists since the only 1-metre separation was insufficient. Despite this limitation, the theoretical framework rigorously establishes the important relationship between Bell nonlocality and genuine randomness, providing the fundamental mathematical bases for all subsequent work.

2.2. Event-Ready Entanglement Scheme with NV Centers

Compared to Pironio, Hensen et al. closed both loopholes simultaneously using electron spins in NV centres separated by 1.3km. Entanglement was produced through an event-ready protocol that relies on entanglement swapping, with the occurrence of entanglement confirmed by simultaneous detection of photons at an intermediate node.

The detection hole is closed as every heralded event was recorded guaranteed by single-shot spin readout with fidelity >96 %. Moreover, due to fast quantum random number generators and short time window, the spacetime separation is ensured, which closes the locality loophole. A martingale-based hypothesis was applied for statistical analysis which does not assume i.i.d. behavior and allows for memory in the devices. This test produces a p-value that quantifying the probability that a local realist model could explain the observed data. The authors went through 245 valid trials, which obtains a p-value of 0.039.

2.3. High-Efficiency Photonic Bell Test with Clauser-Horne Inequality

Shalm et al. distributed polarization-entangled photon pairs-generated at 1550 nm through SPDC in a Sagnac interferometer to two spatially separated stations around 100 meters apart. They used superconducting nanowire single-photon detectors (SNSPDs) with > 90 efficiency to close the detection loophole. In order to close the locality loophole, the random basis choice (XOR of three independent sources: a phase-diffusion laser, a single-photon sampler, and a pseudorandom source.) was completed before light signals could reach the stations.

Instead of common CHSH inequality, they used Clauser-Horne inequality which is more suitable for photonic experiments with losses:

$$P(++|ab) \leq P(+0|ab') + P(0+|a'b) + P(++|a'b') \tag{2}$$

In details, $P(++|ab)$ represents the probability that both Alice and Bob detect a photon; $P(+0|ab')$ represents Alice detects while Bob does not.

2.4. Spot-Checking Protocol with Entropy Accumulation Theorem

Liu et al. extended the photon-based loophole-free test into a complete DI-QRNG (Digital Independent-Quantum Random Number Generator). To achieve high-efficiency detection, they utilized a spot-checking protocol: most trials used fixed inputs while a small fraction used random inputs to estimate Bell violation. In Liu's experiment, the Bell violation is quantified by the CHSH game value:

$$J = \frac{1}{n}\sum_{i=1}^{n} J_i - 3/4 \tag{3}$$

where $J_i = 1$ if the CHSH condition $ai \oplus bi = xi * yi.$ is satisfied and 0 otherwise. A positive CHSH game value indicates the existence of Bell violation.

Security was built on the entropy accumulation theorem (EAT), providing a lower bound on min-entropy without i.id. assumption:

$$H_{min}^{\epsilon_s}(\mathrm{AB} \mid \mathrm{XYE}) \geq n \cdot R_{opt}(\epsilon_s, \epsilon_{EA}, \omega_{exp}) \tag{4}$$

R_{opt} is the optimal randomness rate per trial, ϵ_s is a smoothing parameter, ϵ_{EA} is the entropy accumulation error, and ω_{exp} is the expected CHSH game value. This framework guarantee security even when an adversary holds quantum side information. As for randomness extraction, a Toeplitz matrix with size of 137.90 Gb × 62.469 Mb is used.

2.5. Chip-Based Heterodyne SDI-QRNG

The author used a source-device-independent framework. For this framework, the measuring apparatus is trusted and characterized. On the contrary, the quantum source is fully controlled by an adversary to make it untrusted. The core component is a heterodyne receiver implemented on a silicon photonic integrated chip (PIC). The chip is used to split the incoming signal into two quadrature, q and p which are detected by balanced photodiodes. The entire module- including PIC, RF electronics, and DC control- fits into 7.5×10×2.5cm.

For a heterodyne receiver with phase-space resolution δ_q and δ_p, Eve's guessing probability is bounded by $P_{guess}(X|E) \leq \frac{\delta_q \delta_p}{\pi}$. The corresponding min-entropy per measurement is:

$$H_{min}(X|E) \geq -\log_2 \frac{\delta_q \delta_p}{\pi} \tag{5}$$

The overall security extends to coherent attacks through tensor-product POVM decomposition, making the bound valid against general quantum adversaries. Randomness is extracted using a Toeplitz matrix (17,600 columns × 11,008 rows).

3. Research Results and Analysis

3.1. Min-Entropy Certification from CHSH Violation

The experiment ran 3,016 trials. They measured the CHSH parameter S. The result was S=2.414±0.058 which is above 2, so it violates the Bell inequality. They used their entropy bound to find how many random bits they had. They certified 42 random bits with 99% confidence. This is not a large number. But it was the first time anyone showed that Bell violation can directly certify randomness. The result was a proof of principle [3].

The theoretical basis for this certification is shown in Figure 1. It plots the min-entropy per trial against the CHSH value S. From the plot, the curve is at zero when $S = 2$. As S increases above 2, the curve rises. This tells that more randomness becomes available when the Bell violation is larger. The figure also includes three different curves: the tightest one comes from quantum theory, while the others come from simpler approximations. For the measured value S = 2.414, the curve gives a positive entropy. Multiplying this per-trial value by the number of trials gives the 42 certified bits.

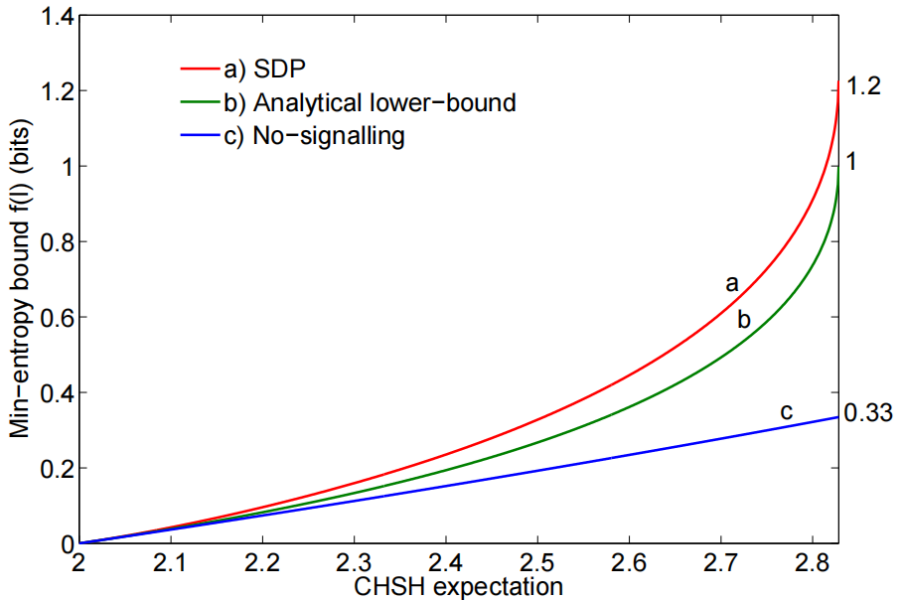

Fig. 1 Min-entropy per trial versus CHSH value S [3].

The result was just a proof of principle, not a practical quantum random number generator. However, it provides the theoretical knowledge base for further practical application.

Shalm et al. conducted 245 valid trials with measured $S = 2.42 \pm 0.20$ which demonstrates violation of CHSH inequality. A p-value of 0.039 is obtained under a martingale-based hypothesis test. This is below the standard 0.05 significance threshold, meaning local realism is rejected [5]. Although p-value is only marginally significant, yet this was the first experiment that close both detection and locality loopholes simultaneously, which gives the experimental proof of Bell's theorem. The experimental results show the measured correlations and p-values obtained from both the conventional and complete statistical analyses.

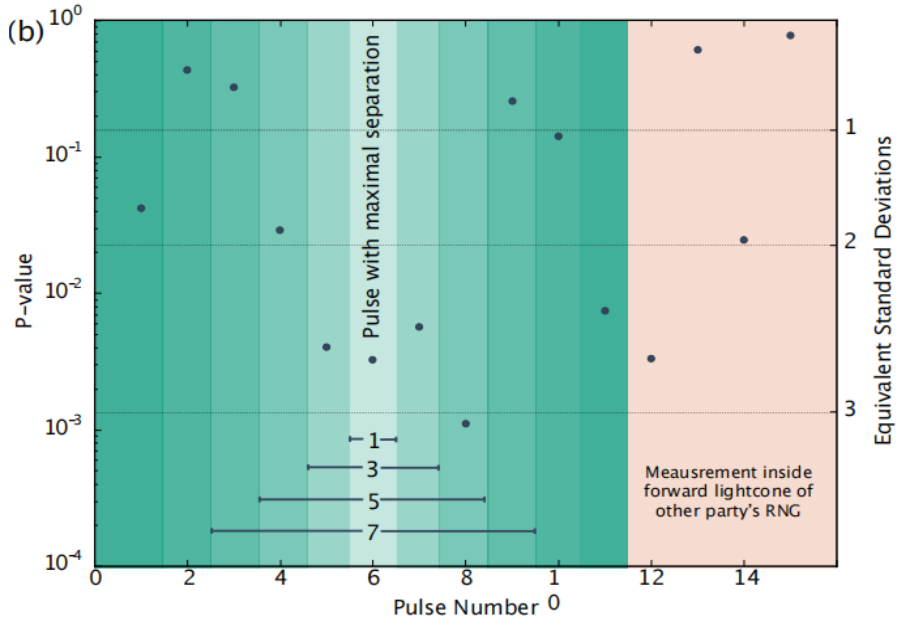

Fig. 2 The *p*-values for 15 individual time slots (blue bars) and aggregate pulse combinations (orange markers) [6].

3.2. High-Confidence Photonic Bell Test

Shalm et al. combined multiple time slots to achieve higher event rate [6]. The resulting p-values for single-pulse, three-pulse, five-pulse, and seven-pulse aggregates are shown in Figure 2. For the five-pulse aggregate, the p-value was very small: 5.9×10^{-9}, which providing overwhelmingly strong evidence against local realism.

They also checked the freedom-of-choice loophole. They added an excess predictability $\epsilon=3\times10^{-3}$. Even with this adjustment, the p-value was only 2.3×10^{-7}. This is still far below 0.05, which indicates the local realism is extremely unlikely. These results can be seen directly from figure 2 which plots the measured correlations across the four measurement settings against the local realism bound. Compared with the NV-centre system, the photon-based method achieved a much higher event rate. In that case, although both of them obtained similar results of P-value, the statistical significance of Shalms's experiment is higher than Hensen's experiment.

3.3. Full DI-QRNG with High-Speed Randomness Extraction

Liu ran $n = 6.895 \times 10^{10}$ trials in 96 hours. The CHSH game value was $J=2.757\times10^{-4}$. This positive value shows Bell violation [7]. Using the entropy accumulation theorem, they found the amount of extractable randomness. They extracted 6.2469×10^{7} random bits at a generation rate of 181 bits per second.

The relationship between the number of trials and extractable randomness is illustrated in Figure 3. As shown, the extracted randomness grows with the trial count and asymptotically approaches the ideal i.i.d. limit. With $n = 6.895 \times 10^{10}$ trials, the experiment reached approximately 56.9% of this asymptotic optimum. Moreover, the extracted bit stream passed the NIST statistical test suite, confirming its uniformity.

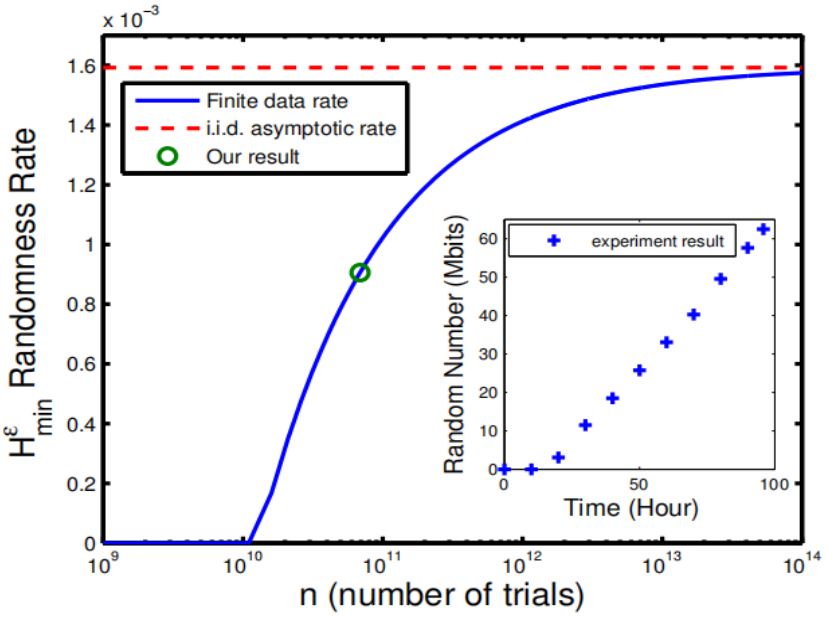

Fig. 3 Extracted randomness versus number of experimental trials [7].

3.4. Chip-Based SDI-QRNG with >20 Gbps Generation Rate

At the maximum local oscillator power (21 mW), the calibrated phase-space resolutions gave a quantum conditional min-entropy of 10.106 ± 0.005 bits per 16-bit sample. With a post-processing sampling rate of 2 GSps, this translates to a secure generation rate of >20 Gbps-—the fastest Semi-DI QRNG reported to date and the first source-device-independent QRNG implemented on a chip.

Under LO power, the measured vacuum-state purity reached 0.883 ± 0.003, with quadrature variances of $\sigma_q^2 = 0.5317$ and $\sigma_p^2 = 0.5347$—close to the ideal vacuum value of 0.5. The author converted 50GB of raw data into 2.5GB of secure random bits. Moreover, the extracted bits passed all NIST statistical tests. The entire module only occupies 7.5 × 10 × 2.5 cm.

4. Conclusion

This analysis has seen how the development of DI and semi-DI Quantum Random Number Generators (QRNGs) has been followed by reviewing five important experimental steps in the period 2010-2025. The story is clear: it goes from the theoretical proof of randomness by using Bell inequalities, to the first Bell tests free of loopholes, to a fully DI QRNG, and finally to a chip based semi-DI that works at speeds above 20 Gbps. This is a dramatic of five orders of magnitude with respect to the DI approach. This evolution shows such a general compromise: the more stringent the requirement of security, the more difficult the experiment and the lower the speed of generation. By easing the requirement of security one can have a practical and high speed of operation, but still with a good robust certification. The full DI gives the most security, but the experimental complicity and the constrained speed makes the real application difficult. The Semi-DI frameworks offer an attractive compromise, easing certain assumptions while still ensuring stringent certification.

Looking ahead, routed Bell experiments and self-testing approaches are expected to improve both the operational range and the performance efficiency. On the other hand, the point of chip-scale integration is of modules that can be used in the real world. In the same respect, the application of the idea of Bell-based verification to quantum key distribution shows that the wider the relevance of these methods is not only for quantum random number generator. One expects that the hybrid device-independent-semi-device-independent designs, plus the use of integrated photonic platforms, will help to move the verified quantum randomness from the experimental set up into the functional cryptographic system that will satisfy the increasing need of randomness reliable in a world of e growing digital connectivity.

References

[1] Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. Rev Mod Phys. 2017;89(1):015004.

[2] Crumpler NR, Chandra V, Zakamska NL, et al. Detection of the Temperature Dependence of the White Dwarf Mass–Radius Relation with Gravitational Redshifts. Astrophys J. 2024;977(2):237.

[3] Pironio S, Acín A, Massar S, et al. Random numbers certified by Bell's theorem. Nature. 2010;464(7291):1021-1024.

[4] Zhang Y, Shalm LK, Bienfang JC, et al. Improved device-independent quantum random number generation with a loophole-free Bell test. Phys Rev Lett. 2022;128(11):110505.

[5] Hensen B, Bernien H, Dréau AE, et al. Loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km. Nature. 2015;526(7575):682-686.

[6] Shalm LK, Meyer-Scott E, Christensen BG, et al. Strong loophole-free test of local realism. Phys Rev Lett. 2015;115(25):250402.

[7] Liu Y, Zhao Q, Li MH, et al. Device-independent quantum random-number generation. Nature. 2018;562(7728):548-551.

[8] Bertapelle T, Avesani M, Santamato A, et al. High-speed source-device-independent quantum random number generator on a chip. Optica Quantum. 2025;3(1):111.

[9] Nadlinger DP, Drmota P, Nichol BC, Arlt G, Lucas DM. Experimental quantum key distribution certified by Bell's theorem. Nature. 2022;607(7920):682-686.

[10] Gigena N, Panwar E, Scala G, Araujo M, Farkas M, Chaturvedi A. Self-testing tilted strategies for maximal loophole-free nonlocality. npj Quantum Inf. 2025;11(1):82.