ARTICLE

Check for updates

Quantum random number generation based on a perovskite light emitting diode

Joakim Argillander [1], Alvaro Alarcón [1], Chunxiong Bao [2,3], Chaoyang Kuang [2], Gustavo Lima [4,5], Feng Gao [2✉] & Guilherme B. Xavier [1✉]

The recent development of perovskite light emitting diodes (PeLEDs) has the potential to revolutionize the fields of optical communication and lighting devices, due to their simplicity of fabrication and outstanding optical properties. Here we demonstrate that PeLEDs can also be used in the field of quantum technologies by implementing a highly-secure quantum random number generator (QRNG). Modern QRNGs that certify their privacy are posed to replace classical random number generators in applications such as encryption and gambling, and therefore need to be cheap, fast and with integration capabilities. Using a compact metal-halide PeLED source, we generate random numbers, which are certified to be secure against an eavesdropper, following the quantum measurement-device-independent scenario. The obtained generation rate of more than 10 Mbit s^{-1}, which is already comparable to commercial devices, shows that PeLEDs can work as high-quality light sources for quantum information tasks, thus opening up future applications in quantum technologies.

[1] Department of Electrical Engineering, Linköping University, 581 83 Linköping, Sweden. [2] Department of Physics, Chemistry, and Biology (IFM), Linköping University, Linköping 581 83, Sweden. [3] National Laboratory of Solid State Microstructures, School of Physics, Nanjing University, Nanjing 210093, China. [4] Departamento de Física, Universidad de Concepción, 160-C Concepción, Chile. [5] Millennium Institute for Research in Optics, Universidad de Concepción, 160-C Concepción, Chile. ✉email: feng.gao@liu.se; guilherme.b.xavier@liu.se

The recent development of perovskite photonic devices has had significant impacts in many fields due to their optical properties and low-cost fabrication[1,2]. Perovskites kick-started a revolution as the building material for efficient solar cells[3], while more recently they are also showing great promise for the fabrication of efficient light-emitting diodes (LEDs)[4]. Perovskite LEDs (PeLEDs) that operate at room temperature have already been developed[5], opening up the path for practical perovskite-based light sources. These devices have the potential to be a game changer in fields such as next-generation displays[6], general-purpose lighting[7] and optical communications[8], because PeLEDs possess narrow emission width and widely tunable bandgap, further motivating their use as practical devices[2,6]. Another key advantage is that the fabrication process of perovskite devices can be solution-processed under ambient conditions, for example through spin-coating or inkjet printing. This allows the: (i) integration of perovskite photonics with complementary metal-oxide semiconductors without relying on epitaxial growth and opens up for emerging technologies in wearable, implantable and portable electronics; and (ii) a simpler manufacturing process, which is highly attractive due to a lower associated cost[9,10]. Finally, recent results show advantages in the life cycle assessment of perovskite photovoltaic cells compared with a silicon benchmark in terms of reduced energy payback time and reduced greenhouse gas emission factor[11,12], thus pointing out that PeLEDs might also have similar advantages in their life cycle assessment when compared with standard semiconductor solid-state devices, already pointing towards a more sustainable photonics industry.

The field of quantum information is largely dependent on technological advances provided by other areas in engineering and natural sciences. We have known for decades that the use of quantum systems for information processing opens up previously unreachable results such as carrying out some computation tasks under practical time[13] and the demonstration of the non-local behaviour of nature[14]. However it was not until very recently that experimental demonstrations of a quantum advantage in computing[15,16] and conclusive non-locality tests[17] could be demonstrated. Major advances pushing forward many new applications in photonic quantum technologies include highly efficient single-photon detectors[18], integrated photonic circuits[19] and novel optical fibre designs[20]. Some preliminary efforts have been made in order to use perovskite devices for quantum optics[21,22]. However, perovskite-based devices are yet to be demonstrated in a complete quantum information processing task.

In our work we employ a metal-halide PeLED as the light source for a quantum random number generator (QRNG), providing a radical departure from the usual approach where solid-state light sources are usually employed (semiconductor LEDs or lasers) in quantum technology applications. The generation of random numbers based on the outputs from measurements of quantum systems is highly attractive for practical applications, due to the unavoidably random nature of quantum processes[23]. These numbers are used for a wide variety of applications, from encryption, on-line gaming and gambling, to computer simulations. Here we are able to produce a high-quality stream of random numbers from projective measurements on weak coherent polarisation states produced from the PeLED. The random bits are certified by the widely adopted National Institute of Standards and Technology (NIST) randomness test suite[24]. Simultaneously, we resort to the measurement device-independent (MDI)[25] approach to certify the amount of private randomness that our system can produce in the hypothetical case that our detectors could be compromised by an eavesdropper. The MDI approach is of high relevance for QRNGs as the detectors are the devices that are most prone to being hacked by

side-channel attacks[26]. Our demonstration on the use of PeLEDs for quantum information processing can enable future developments in quantum technologies with perovskite light sources.

Results

Intuitively, randomness is associated with the difficulty of characterising the evolution of all the parameters leading to a given complex process. This is the basic concept behind many commercial random number generators. Nonetheless, from a more stringent perspective of cryptography, it is desired that the privacy of the generated randomness can be certified even against an eavesdropper that has some extra knowledge of the device inner-workings and infinite computational power to analyse the data generated[27]. This is only possible within the framework of quantum mechanics while exploiting the intrinsic randomness of the results of a quantum measurement[28]. QRNGs are usually classified in terms of the amount of assumptions needed by the user to guarantee the privacy of the generated random bits against a malicious eavesdropper. QRNGs based on the modern device-independent (DI) approach provide the ultimate level of security, guaranteeing private randomness even against an eavesdropper that has fabricated the device itself[29–34]. However, the requirements are quite demanding and they can only achieve modest random number generation rates. On the other end of the security spectrum lie standard device-dependent (DD) QRNGs that are capable of producing high random bit generation rates, but where full characterisation of the entire system is needed[35–39]. Solutions based on reasonable assumptions about partial knowledge of the device, the so-called semi-device-independent (SDI) approaches[40], are the new trend for randomness generation as a high output throughput can be achieved with a higher level of security compared to traditional QRNGs[41–52]. Another important class of QRNGs is based on homodyne detection which are capable of ultra-high randomness generation rates and have also been demonstrated in both DD[53,54] and SDI[55–57] classes.

These quantum random number generators represent an important breakthrough in physics and are strong contenders to replace the ones being used today in industry and academia. Nonetheless, this will only be possible if they are made compact, have low manufacturing cost, and can be integrated with other systems. If they are to be mass-produced, then the environmental footprint also becomes important. The use of PeLEDs for building modern QRNGs is highly relevant since they can already satisfy some of these requirements. We gather the generated raw bitrate of the previously mentioned QRNGs in Fig. 1, separated by security class, showing clearly that our result is already highly competitive.

The highly secure measurement-device independent (MDI) QRNG protocol, which belongs to the SDI class, can remarkably certify private randomness even in the case that the detectors are under the control of an eavesdropper[25,40]. In the MDI scenario, a user in need of random numbers possesses a characterised state preparation device (**P**) but has to use an untrusted measurement device (**M**) (Fig. 2a). This scenario has become of upmost practical relevance nowadays, as a side-channel attack to the detectors is the most common strategy for hacking quantum technologies[26]. The basic idea is that **P** now works actively, by randomly preparing different states. One of the states is conventionally used for randomness generation, while the others will be used to check the measurement device. The randomness generation rate is only slightly affected because the testing states can be chosen seldom, and most of the experimental run will still be used for randomness generation. For instance, in our case the state $1/\sqrt{2}(|H\rangle + i|V\rangle)$ is used for randomness generation and the states $|H\rangle$ and $|V\rangle$ will be the testing ones. Whenever the state
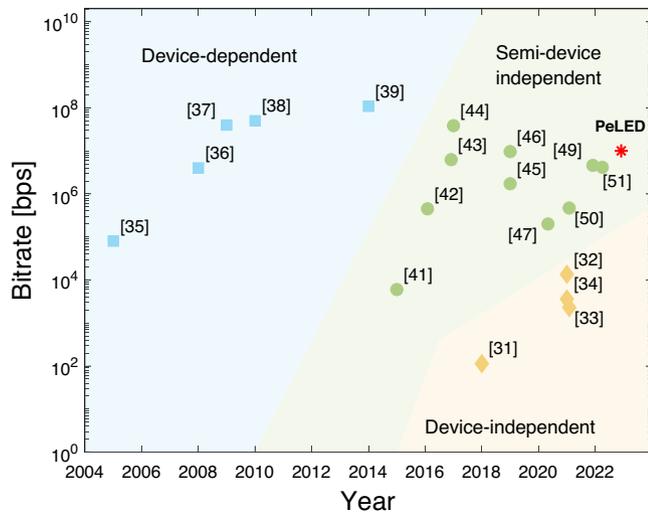
Fig. 1 Raw random bit generation rate of several quantum random number generators as a function of published year. The results are limited to those that employed single-photon detectors and are based on discrete variable quantum systems for direct comparison purposes. Our maximum sustained raw bit rate is 10.35 Mbit s^{-1}.

$|H\rangle$ ($|V\rangle$) is sent, only detector D_1 (D_2) should fire. Remarkably, from the success probabilities of recording the test states one can put an upper bound on the knowledge an eavesdropper can have about the generated random bit sequence. Formally speaking, and assuming the notation of[48], the preparation device is used to randomly prepare a state of a set, $\{\omega_x\}$, with $x = \{0, 1, 2\}$, which are measured by **M**, resulting in an outcome a. After several iterations, one estimates the probabilities $p(a|\omega_x)$. The maximal probability $P_g(x^*)$ of the eavesdropper guessing the outcome a for a given input x^*, compatible with $p(a|\omega_x)$, is given by the solution to a simple numerical optimisation program defined in[25,48]. Note that the eavesdropper aside of having control of the detectors, is allowed to even resort to quantum entanglement for guessing the outcomes a[48]. Finally, the amount of private randomness that is certified per experimental round in the MDI scenario is given by the min-entropy: $\mathcal{H}_{\min}(x^*) = -\log_2 P_g(x^*)$.

Perovskite LED device. The structure of our PeLED is based on an indium tin oxide (ITO)-coated glass substrate (Fig. 2b, c). The active layer consists of formamidinium lead iodide perovskite, with approximately 50 nm thickness. This layer is sandwiched between the electron and hole transport layers which consist of polyethylenimine ethoxylated (PEIE)- modified zinc oxide (ZnO) and poly(9,9-dioctylfluorene-co-N-(4-butylphenyl)diphenyla-mine) (TFB) (~40 nm). They are followed by layers of molybdenum oxide (MoOx) (~7 nm) and gold (~80 nm) as the contact layer. In order to obtain highly stable PeLEDs, we used an additive of pimelic acid (PAC)[58]. Under forward bias, electrons and holes injected into the perovskite layer recombine, efficiently generating photons with a central wavelength of 804 nm, with a spectral width of 41.6 nm full-width at half-maximum with a peak external quantum efficiency of around 18% (see Supplementary Notes 1–3 for further details).

MDI-QRNG Experiment. Our MDI-QRNG is schematically depicted in Fig. 2a. For each measurement round, the user chooses whether to prepare and send the test states, represented by horizontal or vertical polarisation states ($\omega_0 = |H\rangle$ and $\omega_1 = |V\rangle$), or a linear superposition of both test states ($[\omega_2 = |R\rangle = 1/\sqrt{2}(|H\rangle + i|V\rangle)]$) as the random number generation state. The states are
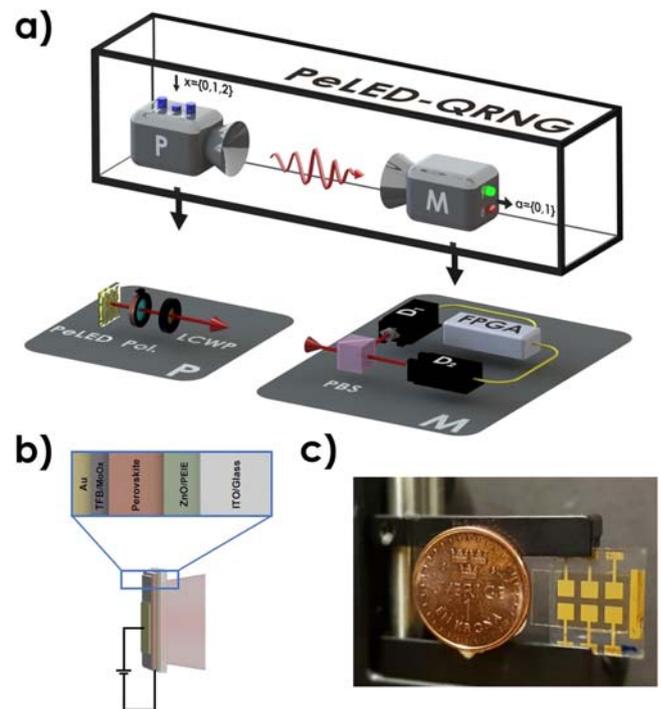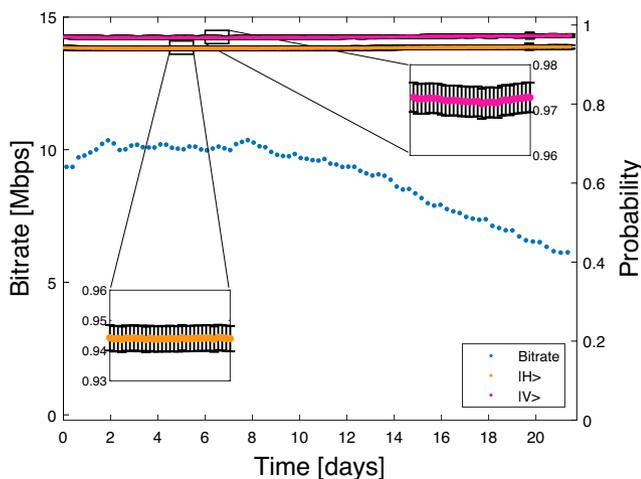

Fig. 2 Experimental setup and perovskite light emitting diode (PeLED) structure. a Scheme of our measurement-device-independent quantum random number generator. On the left the preparation stage (**P**) creates the quantum states to be prepared depending on the user's choice of test or randomness generation states, while a measurement stage (**M**) produces the outputs "0" or "1" for each measurement round. The PeLED is housed inside the preparation stage, where it is used to produce weak coherent states. When the user decides to generate a random number, the superposition state $|R\rangle = 1/\sqrt{2}(|H\rangle + i|V\rangle)$ is prepared with a fixed linear polariser followed by a liquid crystal waveplate. In order to verify the functioning of the measurement device, the user randomly chooses to prepare one of the test states $|H\rangle$ or $|V\rangle$ by electrically controlling the retardance of the waveplate. In our implementation the measurement device consists of an uncharacterised polarising beam splitter (PBS), which in principle should project the incoming states onto the orthogonal states $|H\rangle$ and $|V\rangle$. The outputs of the PBS are connected to single-photon detectors D_1 and D_2. The outcomes "0" or "1" of (**M**) are read by field programmable gate array (FPGA) electronics. **b** The structure of the employed perovskite diodes, with the biasing circuit indicated. The structure shows the stackup of ITO/Glass (indium tin oxide), ZnO/PEIE (polyethylenimine ethoxylated zinc oxide), perovskite, TFB/MoOx (poly(9,9-dioctylfluorene-co-N-(4-butylphenyl)diphenylamine/ molybdenum oxide)) and gold (Au). **c** Close-up photo of one of the PeLED samples mounted on an opto-mechanical mount. A coin worth one Swedish Crown (SEK) placed as a size reference.

produced from weak coherent states of light generated by the PeLED, which is housed in the preparation stage. A linear polariser is employed to filter out the unpolarised light produced by the PeLED before passing through a liquid crystal waveplate (LCWP) with a switching time of less than 50 ms, which is the element employed by the user to implement the choice of ω_x. A ball lens with 50 mm focal length is used to collimate the light emitted from the PeLED, and a calibrated optical attenuator is needed to adjust the mean photon number per detection window, such that the probability to have multi-photon events at the single-photon detectors is negligible ($< 0.28\%$). Both components are omitted for the sake of simplicity. In the MDI framework, the measurement stage is considered as a black box, which is able to output a signal "0" or "1" depending on the measurement result. Nothing else

needs to be assumed about the measurement procedure to certify the privacy of the generated random numbers. In our implementation, the projection of the prepared states is done with an uncharacterised polarising beam splitter (PBS), which in principle should have the horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarisation states associated to the output signals "0" and "1", respectively (see Fig. 2a). The measurement procedure is concluded with silicon single-photon avalanche detectors D_1 and D_2 (Perkin Elmer), with 25% overall detection efficiency at 800 nm. The output "0" or "1" of the measurement stage is registered by field programmable gate array (FPGA) electronics, whose output is then continuously streamed to a personal computer for storage and randomness extraction (see Methods). In the event that neither detector records the presence of a photon (for example due to absorption), that detection event is discarded and not stored. Similarly, if both detectors record the presence of a photon (either from noise in the detectors, from photons from the environment that couple to the fibres, or from multiphoton events) that detection event is also discarded.

In our experiment, before each measurement data block, a decision is randomly taken on whether that block will be used for randomness generation or to test the measurement device, as required in the MDI QRNG protocol[48]. For demonstration purposes in our experiment, the user choice is provided by an external software-based random number generator, with a bias of 99% towards randomness generation mode. In more sensitive applications, the user needs to have a trusted low-rate source of randomness, or use a small fraction of bits generated as feedback for the choice of measurement block type, while also saving some bits for a new session. Please note that any source of randomness may be used, even the partial output of a previous run or another source the user trusts. In Fig. 3 we display the raw bit generation rate as a function of elapsed time of the experiment, where one can see that it attains a remarkably high maximal value of 10.35 Mbit s^{-1} between days 2 and 8 approximately, and an

average of 9.01 ± 1.30 Mbit s^{-1} over the entire run. We observe stable performance approximately in the first 8 days, and then a slow decay due to degradation of the PeLED, with a constant current density applied of 0.24 mA cm^{-2}. Nevertheless after 22 days, the PeLED still has more than half of its original brightness. We also display the success probabilities recorded for either the $|H\rangle$ or $|V\rangle$ test states, when activated by the user, during the whole measurement run. Please note that the user switches seamlessly between the transmitted states with the liquid crystal waveplate. The overall random number generation rate does not suffer a penalty, since the test states are only used 1% of the time. In spite of the fact the emission rate from the PeLED deteriorates, there is no change in the success probability for the test states, showing there is no change in the certification of the privacy of the random numbers generated. The difference for the measured probabilities between both states, is from the different transmission/reflection coefficients of the polarising beam splitter in the **M** stage. The average success probability for the entire generated random bit sequence is $P_{suc} = 0.97 \pm 0.01$. This places an upper bound on the randomness generated per experimental round that is certified to be private against detector side-channel attacks. In our particular implementation it corresponds to $\mathcal{H}_{min} = 0.71 \pm 0.01$ random bits, which is quite high considering the innovative aspects of our QRNG.

Randomness assessment. Following the Toeplitz randomness extraction procedure we test the randomness of the final random bit key. Initially, we plot the first 0.5 Mbit of the generated sequence as an image where every 8-bit grey-level pixel is encoded directly from the random sequence (Fig. 4a). We choose only a small subset in this example due to limitations in displaying the entire data as a single image with reasonable size. Nevertheless, one can clearly observe the randomness of the data as the figure is indistinguishable from noise. Then a randomly selected 5 Gbits of the entire generated random bit sequence is fed to the NIST randomness statistical test suite, a well-known benchmark for statistically certifying the randomness of a sequence[24]. The test suite consists of 16 tests (listed in Fig. 4b, c), and for each test the original sequence is divided into b blocks of equal size. A typical block size is 1 million bits, which we have employed. The test result is a numerical value between 0 and 1 called a p-value, and a test is considered a pass if the corresponding result is above the confidence value of $\alpha = 0.01$. Figure 4b shows the average of the p-values for all data blocks in each test with the corresponding standard deviation, clearly showing the generated sequence passes all tests. Furthermore in Fig 4c we plot the proportion of blocks in each test that passes with a p-value greater than 0.01. Also shown is the confidence level for the minimum proportion of tests that must pass in order to ensure randomness certification for the bit sequence (see "Methods": Statistical testing).


Fig. 3 Performance of the quantum random number generator with a perovskite light emitting diode (PeLED). Random number generation rate as a function of elapsed experiment time. Each blue dot corresponds to the average rate over 6 hours, and we obtain an overall average of 9.01 ± 1.30 Mbit s^{-1}, with a maximum sustained rate of 10.35 Mbit s^{-1}. Also shown are the probabilities to measure either the $|H\rangle$ or $|V\rangle$ test states, as required to test of the measurement device in the MDI protocol. Each test state is randomly chosen by the user with a 0.5% chance at the beginning of every measurement block. The insets show a higher time resolution sample of each test state data. Error bars come from assuming Poissonian statistics of the PeLED photon number distribution combined with the detection process.

Conclusion

Perovskites have played a major role in the development of highly-efficient solar cells, thus greatly pushing solar power plants into becoming a major player in the production of electricity worldwide. The recent development of optoelectronic devices from perovskites is opening up the field of photonics for this material. PeLEDs are poised to have significant impacts in the areas of solid-state lighting and optical communications, with its lower carbon footprint during its entire life cycle as well as optical and mechanical properties being major motivators for their use. These properties are extremely attractive to the blooming field of quantum technologies, specifically aiming towards the widespread deployment of applications, even down to the consumer level. Following this direction, we have showed that PeLEDs can
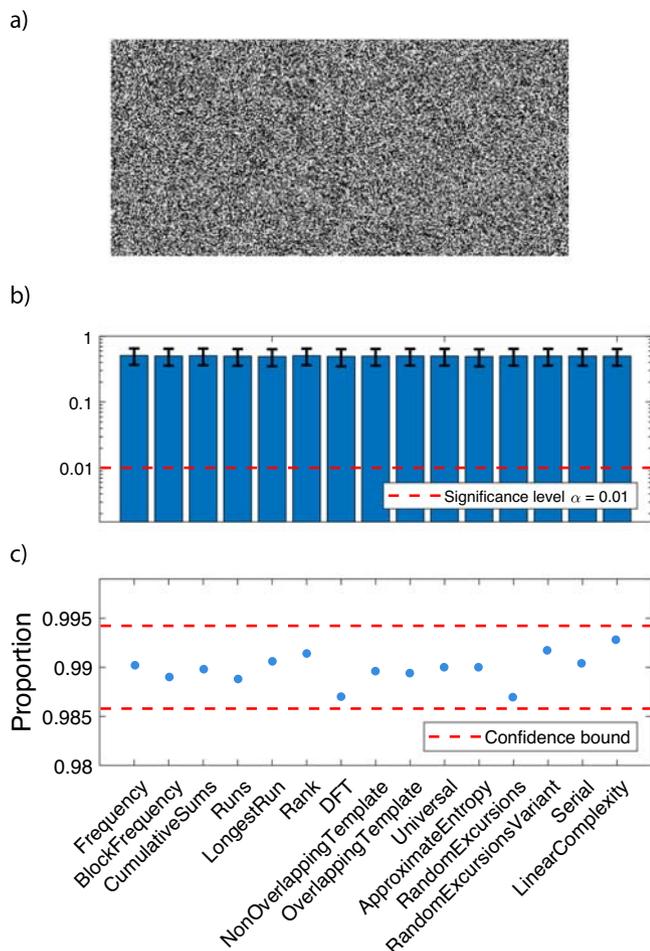
Fig. 4 Quantum random number generation with perovskite light emitting diodes (PeLEDs). a Sequence of generated random bits (0.5 Mbit in length) plotted as an image, where each pixel has an 8-bit grey-scale colour depth. **b** Results of the NIST statistical test suite on 5 Gbits of the generated random sequence. Each of the sixteen tests of the suite is labelled on the x-axis, and on the y-axis is the numerical result for each test from 0 to 1, called the p-value. We employ a standard confidence value of 0.01, meaning a test is considered successful if its p-value above this number. Displayed are the average results of each test, with the standard deviation of the test results. **c** Here we plot the proportion r of passed runs within each test. The significance level for a test to be considered passed is shown in the graph as the dashed red line ("Methods": statistical testing).

be successfully employed to implement modern and highly secure quantum random number generation protocols. Our results (Fig. 1) place our QRNG among the best reported, including commercial devices[59], and thus show the feasibility of quantum technology systems with perovskite light sources, while also pointing towards initiatives to make the quantum technology industry more sustainable. We successfully demonstrated that the generated sequence passes the stringent NIST randomness test suite, a widely recognized benchmark employed for the certification of randomness in a sequence of numbers. At the same time, we have also guaranteed the privacy of at least 71% of the generated random numbers by implementing our QRNG with the MDI approach. We have obtained an operational lifetime of at least 22 days for the developed PeLED, given that the device had not yet quite reached half of its initial brightness. While this result is very high for a PeLED[60], recent works have shown new solutions to further increase the operational stability[61,62], thus

showing a viable path for PeLEDs to be used in QRNGs for practical applications.

Methods

Randomness extractor and data streaming. The generated raw bit sequence is buffered in the FPGA in blocks of 2^{16} bits before they are streamed over a UDP protocol to a host computer acting as server for final storage. The server then stores the acquired data for each of the different states separately to facilitate (i) security analysis, and (ii) randomness extraction. We then generate close to perfectly uniform sequences of numbers by applying a Toeplitz hashing extractor to the generated raw bits recorded for the experiment rounds where the prepared state was |R⟩. We first split the raw binary sequence into N sequences of length n which we then multiply with an $n \times m$ Toeplitz matrix to generate an output of m hashed bits, following the procedure in[63]. Therefore we employ $n = 400$, and m is given by $m = \mathcal{H} - 2\log_2\varepsilon$ where $\mathcal{H} = -\log_2[\max_{x\in\{0,1\}^8} \Pr\{X = x\}]$ is the minimum entropy when considering binary strings of length 8, and $\varepsilon = 2^{-100}$ is a security parameter derived from the leftover hash lemma[63].

The Toeplitz matrix T is defined at the beginning of the extraction procedure using a seed of $n + m - 1$ bits taken from the beginning of the raw sequence. These bits specify the elements of the first row and column of the matrix. As T can be reused for each of the subsequences, we obtain the final extracted sequence by concatenation of the results of the matrix multiplications $Tn_1, Tn_2, \ldots, Tn_N$, where the subscript indicates the sequence number[63,64].

Statistical testing. For each of the tests in the NIST 800-22 suite we compute the proportion r of sequences that yielded a p-value greater than the significance level $\alpha = 0.01$[24]. We employ a confidence interval for the proportion of passed tests as $r \pm 3\sqrt{\frac{\alpha(1-\alpha)}{b}}$, as defined in[24], where $b = 5000$ is the number of sequences fed to the test. This results in a confidence interval of $0.9858 \le r \le 0.9942$, where we consider a test passed if the proportions of sequences with p values $p_i{\ge}\alpha$ fall within the interval.

Data availability
The data that support the findings of this study are available from the corresponding authors on reasonable request.

Code availability
The program code that supports the findings of this study is available from the corresponding authors on reasonable request.

References
1. Sutherland, B. R. & Sargent, E. H. Perovskite photonic sources. *Nat. Photon.* **10**, 295 (2016).
2. Zhang, Q., Diederichs, C. & Xiong, Q. Golden hour for perovskite photonics. *Photon. Res.* **8**, PP1 (2020).
3. Kojima, A., Teshima, K., Shirai, Y. & Miyasaka, T. Organometal halide perovskites as visible-light sensitizers for photovoltaic cells. *J. Am. Chem. Soc.* **131**, 6050–6051 (2009).
4. Liu, X.-K. et al. Metal halide perovskites for light-emitting diodes. *Nat. Mater.* **20**, 10 (2021).
5. Tan, Z.-K. et al. Bright light-emitting diodes based on organometal halide perovskite. *Nat. Nanotechnol.* **9**, 687–692 (2014).
6. Quan, L. N. et al. Perovskites for next-generation optical sources. *Chem. Rev.* **119**, 7444–7477 (2019).
7. Bidikoudi, M., Fresta, E. & Costa, R. D. White perovskite based lighting devices. *Chem. Phys.* **54**, 8150 (2018).
8. Bao, C. et al. Bidirectional optical signal transmission between two identical devices using perovskite diodes. *Nat. Electron.* **3**, 156–164 (2020).
9. Ren, A. et al. Emerging light-emitting diodes for next-generation data communications. *Nat. Electron.* **4**, 559–572 (2021).
10. Vasilopoulou, M. et al. Advances in solution-processed near-infrared light-emitting diodes. *Nat. Photonics.* **15**, 656–669 (2021).
11. Tian, T., Stranks, S. D. & You, F. Life cycle energy use and environmental implications of high-performance perovskite tandem solar cells. *Sci. Adv.* **6**, eabb0055 (2020).
12. Tian, T., Stranks, S. D. & You, F. Life cycle assessment of recycling strategies for perovskite photovoltaic modules. *Nat. Sustainability* **4**, 821 (2021).

13. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124-134 (1994) https://doi.org/10.1109/SFCS.1994.365700.

14. Bell, J. S. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195–200 (1964).

15. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).

16. Zhong, H.-S. et al. Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).

17. Hensen, B. kilometres. *Nature* **526**, 682 (2015).

18. Marsili, F. et al. Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7**, 210–214 (2013).

19. Wang, J., Sciarrino, F., Laing, A. & Thompson, M. G. Integrated photonic quantum technologies. *Nat. Photonics* **14**, 273 (2020).

20. Xavier, G. B. & Lima, G. Quantum information processing with space-division multiplexing optical fibres. *Commun. Phys.* **3**, 9 (2020).

21. Zhang, X. et al. Ultrafast two-photon optical switch using single crystal hybrid halide perovskites. *Optica* **8**, 735–742 (2021).

22. Utzat, H. et al. Coherent single-photon emission from colloidal lead halide perovskite quantum dots. *Science* **363**, 1068–1072 (2019).

23. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004 (2017).

24. Rukhin, A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762.

25. Šupić, I., Skrzypczyk, P. & Cavalcanti, D. Measurement-device independent entanglement and randomness estimation in quantum networks. *Phys. Rev. A* **95**, 042340 (2017).

26. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).

27. Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213 (2016).

28. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47**, 595 (2000).

29. Pironio, S. et al. Random numbers certified by Bell?s theorem. *Nature* **464**, 1021 (2010).

30. Bierhorst, P. et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).

31. Liu, Y. et al. High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole. *Phys. Rev. Lett.* **120**, 010503 (2017).

32. Liu, W.-Z. Device-independent randomness expansion against quantum side information. *Nat. Phys.* **17**, 448–451 (2021).

33. Li, M.-H. et al. Experimental realization of device-independent quantum randomness expansion. *Phys. Rev. Lett.* **126**, 050503 (2021).

34. Shalm, L. K. et al. Experimental realization of device-independent quantum randomness expansion. *Nat. Phys.* **17**, 452–456 (2021).

35. Ma, H.-Q., Xie, Y. & Wu, L.-A. Random number generation based on the time of arrival of single photons. *Appl. Optics* **44**, 36 (2005).

36. Dynes, J. F., Yuan, Z. L., Sharpe, A. W. & Shields, A. J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **93**, 031109 (2008).

37. Wayne, M. A. Photon arrival time quantum random number generation. *J. Mod. Opt*. **56**, 516–522 (2009).

38. Fürst, H. et al. High speed optical quantum random number generation. *Opt. Exp.* **18**, 13029–13037 (2010).

39. Nie, Y.-Q. et al. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Appl. Phys. Lett.* **104**, 051110 (2014).

40. Pawłowski, M. & Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A* **84**, 010302 (2011).

41. Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501 (2015).

42. Cao, Z., Zhou, H., Yuan, X. & Ma, X. Source-Independent Quantum Random Number Generation. *Phys. Rev. X* **6**, 011020 (2016).

43. Nie, Y.-Q. et al. Experimental measurement-device-independent quantum random-number generation. *Phys. Rev. A* **94**, 060301(R) (2016).

44. Brask, J. B. et al. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.* **7**, 054018 (2017).

45. Li, Y.-H. et al. Quantum random number generation with uncharacterized laser and sunlight. *npj Quantum Inf.* **5**, 97 (2019).

46. Brask, J. B. et al. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Phys. Rev. Appl.* **7**, 054018 (2017).

47. Rusca, D. Self-testing quantum random-number generator based on an energy bound. *Phys. Rev. A* **100**, 062338 (2019).

48. Cariñe, J. et al. Multi-core fiber integrated multi-port beam splitters for quantum information processing. *Optica* **7**, 542–550 (2020).

49. Mironowicz, P. et al. Quantum randomness protected against detection loophole attacks. *Quantum Inf. Process.* **20**, 39 (2021).

50. Pivoluska, M. et al. Semi-device-independent random number generation with flexible assumptions. *npj Quantum Inf.* **7**, 50 (2021).

51. Zhang, Y. et al. A simple low-latency real-time certifiable quantum random number generator. *Nat. Commun.* **17**, 1056 (2021).

52. Liu, W.-B. et al. Source-independent quantum random number generator against tailored detector blinding attacks. *Opt. Express* **31**, 11292–11307 (2003).

53. Marangon, D. G. et al. Long-term test of a fast and compact quantum random number generator. *Journal of Lightwave Technology* **36**, 3778–3784 (2018).

54. Bruynsteen, C., Gehring, T., Lupo, C., Bauwelinck, J. & Yin, X. 100-Gbit/s integrated quantum random number generator based on vacuum fluctuations. *PRX Quantum* **4**, 010330 (2023).

55. Smith, P. R., Marangon, D. G., Lucamarini, M., Yuan, Z. L. & Shields, A. J. Simple source device-independent continuous-variable quantum random number generator. *Phys. Rev. A* **99**, 062326 (2019).

56. Drahi, D. et al. Certified quantum random numbers from untrusted light. *Phys. Rev. X* **10**, 041048 (2020).

57. Gehring, T. et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. *Nat. Commun.* **12**, 605 (2021).

58. Kuang, C. et al. Critical role of additive-induced molecular interaction on the operational stability of perovskite light-emitting diodes. *Joule* **5**, 618 (2021).

59. https://www.idquantique.com/random-number-generation/products/quantis-qrng-chip/.

60. Kong, L. et al. Stability of perovskite light-emitting diodes: Existing issues and mitigation strategies related to both material and device aspects. *Adv. Mater.* **34**, 2205217 (2022).

61. Guo, B. et al. Ultrastable near-infrared perovskite light-emitting diodes. *Nat. Photon.* **16**, 637–643 (2022).

62. Chen, W. et al. Highly bright and stable single-crystal perovskite light-emitting diodes. *Nat. Photon.*https://doi.org/10.1038/s41566-023-01167-3 (2023).

63. Ma, X. et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).

64. Bing, Q. True randomness from an incoherent source. *Rev. Sci. Inst.* **88**, 113101 (2017).

Acknowledgements

Author contributions

G.X., F.G. and G.L. coordinated the work. C.B., C.K. and F.G. manufactured and characterised the PeLEDs. The measurements were performed by J.A. and A.A. with assistance from G.X. Data analysis was done by J.A. with assistance from G.X. and G.L. All authors contributed to the writing of the manuscript.

Funding

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-023-01280-3.

Correspondence and requests for materials should be addressed to Feng Gao or Guilherme B. Xavier.

Peer review information : *Communications Physics* thanks Xiongfeng Ma and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.

Reprints and permission information is available at http://www.nature.com/reprints