nature photonics

LETTERS

PUBLISHED ONLINE: 29 AUGUST 2010 | DOI: 10.1038/NPHOTON.2010.197

A generator for unique quantum random numbers based on vacuum states

Christian Gabriel[1,2]*, Christoffer Wittmann[1,2], Denis Sych[1,2], Ruifang Dong[1,2,3], Wolfgang Mauerer[4], Ulrik L. Andersen[1,2,3], Christoph Marquardt[1,2] and Gerd Leuchs[1,2]

Random numbers are a valuable component in diverse applications that range from simulations[1] over gambling to cryptography[2,3]. The quest for true randomness in these applications has engendered a large variety of different proposals for producing random numbers based on the foundational unpredictability of quantum mechanics[4–11]. However, most approaches do not consider that a potential adversary could have knowledge about the generated numbers, so the numbers are not verifiably random and unique[12–15]. Here we present a simple experimental setup based on homodyne measurements that uses the purity of a continuous-variable quantum vacuum state to generate unique random numbers. We use the intrinsic randomness in measuring the quadratures of a mode in the lowest energy vacuum state, which cannot be correlated to any other state. The simplicity of our source, combined with its verifiably unique randomness, are important attributes for achieving high-reliability, high-speed and low-cost quantum random number generators.

Many popular random number generators (RNGs) are based on classical computer algorithms and have the advantage of being fast and easy to implement. The best examples pass many statistical tests[16–20] and thus seem random. However, they are based on fully deterministic, repeatable patterns of numbers, thus rendering these generators only 'pseudo random'.

Other types of generators are based on the seemingly random measurement outcomes of classically noisy (thermal) systems[21–23]. Such a hardware approach is intrinsically more secure than the software approach, because the measurement of chaotically behaving systems is practically impossible to predict. However, as long as they are purely classical systems, in principle they have a deterministic nature.

In contrast to these classical systems, quantum-mechanical systems offer the ultimate in randomness. Certain measurements of pure quantum observables yield completely random outcomes, as postulated by quantum mechanics. As a simple example, we consider the polarization measurement (in the canonical basis $\{|H\rangle, |V\rangle\}$) of a polarization qubit, $1/\sqrt{2}(|H\rangle + |V\rangle)$, which yields the unbiased and thus completely unpredictable outcomes $|H\rangle$ and $|V\rangle$. Then, by assigning the bit values '0' and '1' to these outcomes, a sequence of truly random numbers can be generated.

Although random, it is not possible from these tomographically incomplete measurements to conclude whether the numbers are unique. If an attacker takes control over the source and randomly produces $|H\rangle$ and $|V\rangle$, the generated numbers would also be random but perfectly correlated with those of the attacker. Ways of excluding a possible attack and thus ensuring the generation of unique random numbers include using a measurement strategy that is tomographically complete[12] or a detection-loophole free Bell test[13]. From such measurements, the purity of the state can be computed and the possible correlation to an adversary can be determined. In the case where the measured state is pure, the random numbers are unique[15]. We note, however, that this is only valid if all attacks on the classical parts of the system such as the detectors or the classical computer memory can be prevented. We trust these classical security aspects and would here like to focus only on the quantum-mechanical security considerations.

In this Letter, we propose and experimentally implement a quantum RNG producing unique random numbers by exploiting the quantum uncertainty of continuous quantum observables, the quadrature amplitudes, of the vacuum state. We use a very simple homodyne detector, an optimized bit conversion method and a hashing function to produce unique random numbers at low cost and maximum speed. The uniqueness of the random numbers is ensured by the inherent purity of the vacuum state, which cannot be controlled by an attacker.

We consider the quadrature measurement of the vacuum state, which in the quadrature (or equivalently the position) representation can be written as

$$|0\rangle = \int_{-\infty}^{\infty} \psi(x)|x\rangle \mathrm{d}x$$

where $|x\rangle$ are the amplitude quadrature eigenstates ($\langle x|x'\rangle = \delta(x - x')$) and $\psi(x)$ is the ground-state wavefunction, which is a Gaussian function centred around $x = 0$. The measurement of the amplitude quadrature collapses the wavefunction into quadrature eigenstates, and the associated outcomes being unpredictable but biased according to the Gaussian probability function $|\psi(x)|^2$. Unbiased numbers (this is a stringent requirement for the generation of random numbers) can be obtained by binning the measurement outcomes such that the integrated probability associated with each bin is equalized; that is, $\int_{-\infty}^{x_1} |\psi(x)|^2 \mathrm{d}x = \int_{x_1}^{x_2} |\psi(x)|^2 \mathrm{d}x = \cdots = \int_{x_l}^{\infty} |\psi(x)|^2 \mathrm{d}x$, where $l + 1$ is the number of bins. All the measurement outcomes within one bin are assigned a fixed bit combination (Fig. 1b). The length of this bit combination depends on the number of bins; that is for $l + 1 = 2^n$ bins, the length of the bit combination is n.

The quadrature measurement is conducted with a homodyne detector as shown in Fig. 1a. In such a detection system a weak signal (here the vacuum state) and a strong laser beam, called the local oscillator (LO), interfere on a symmetric beamsplitter to form two output beams with balanced powers. The two outputs are measured with two intensity detectors with carefully balanced amplifications, and the resulting electrical currents are digitized,

[1]Max Planck Institute for the Science of Light, Guenther-Scharowsky-Strasse 1, D-91058 Erlangen, Germany, [2]Institute for Optics, Information and Photonics, University Erlangen-Nuremberg, Staudtstrasse 7/B2, D-91058 Erlangen, Germany, [3]Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark, [4]Siemens AG, Corporate Technology, Otto-Hahn-Ring 6, 81739 München, Germany. *e-mail: Christian.Gabriel@mpl.mpg.de

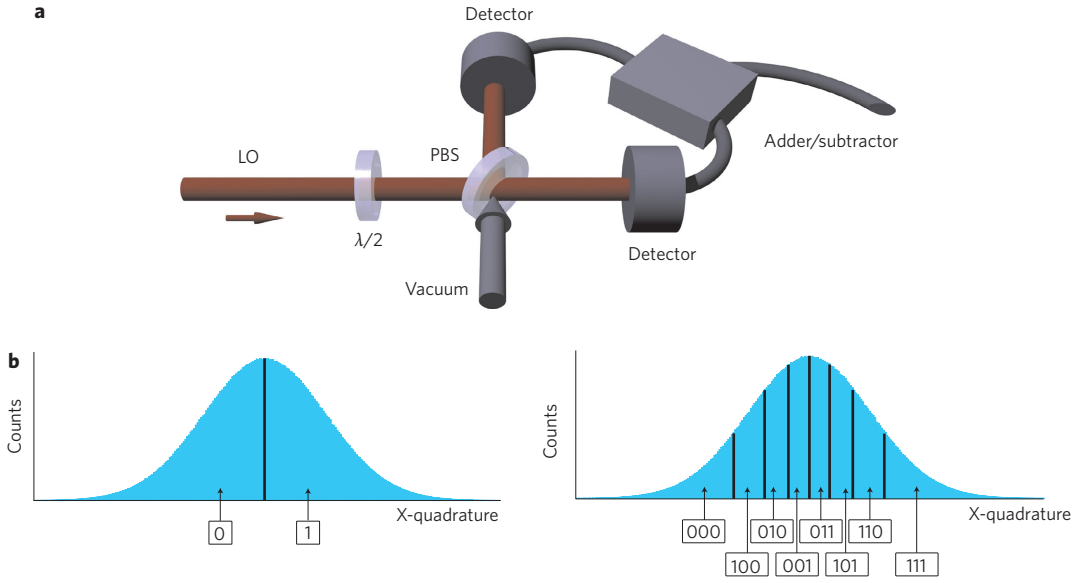

Figure 1 | The homodyne setup, measurement and generation of raw bit sequences. a, The setup consists of a standard laser source generating a local oscillator (LO), a half-wave plate, a polarizing beamsplitter (PBS) and two balanced detectors. Adding or subtracting the photocurrents results in a quadrature measurement of the LO or vacuum state, respectively. **b**, The probability distribution of the vacuum state is binned into 2^n equal parts (the same sample size per bin). The random numbers are then produced by assigning a fixed bit combination of length n to each sample point in a certain bin. Here an example for $n=1$, $n=3$ is shown.

subtracted and fed into a storage element. The difference current is proportional to the quadrature amplitudes of the vacuum state. A plot of the outcomes as a function of time is shown in Fig. 2a, with the statistics shown in Fig. 2b. These outcomes are subsequently divided into different bins, as explained above.

Our quantum RNG (QRNG) includes at least two important features. First, our basic resource for random numbers—the vacuum state—is a particle-free state that cannot be influenced by a potential attacker because the vacuum port of the beamsplitter is blocked. Because of this physical rejection of any input state but the vacuum state, it is guaranteed that a pure quantum state is measured, which in turn renders a tomographically complete measurement unnecessary. Second, the LO does not have to be quantum noise limited, but could have some excess noise, as this noise will be rejected in the balanced homodyne measurement scheme. Therefore, the setup can be realized with widely available commercial products such as standard diode lasers, photodiodes and beamsplitters. The system is thus very robust against external influences and, as a result, it exhibits long-term stability and has the potential to generate random numbers at very high speed.

The total entropy $H(X)_{\text{total}}$ of the bit sequences contains information originating from quantum noise, $H(X)_{\text{quant}}$, but also from classical effects, $H(X)_{\text{class}}$, such as electronic noise and LO noise due to imperfect balancing. The entropy of the quantum-mechanical effects can be calculated as $H(X)_{\text{quant}} = H(X)_{\text{total}} - H(X)_{\text{class}}$. $H(X)_{\text{total}}$ is given by the amount of binning as $H(X)_{\text{total}} = -\sum_{i=1}^{l+1} p_i^{\text{vac}} \log_2 p_i^{\text{vac}}$, where p_i^{vac} is the probability to find a measurement outcome in the ith bin of the $l+1$ bins of the probability distribution of the vacuum state. Analogously, the entropy of the electronic noise can be calculated, which is the major contribution to $H(X)_{\text{class}}$. By also taking into account the LO noise due to imperfect balancing, the classical and therefore also the quantum entropy $H(X)_{\text{quant}}$ can be determined.

Following this protocol for the entropy estimation, we can calculate the effective number of bits (those originating from the quantum entropy) with varying amounts of bins (Fig. 3c). In our QRNG, we use 32 bins (5 bits per sample) as for this value the effective number of bits starts to converge to the maximum information capacity. We find that the entropy of all classical effects is $H(X)_{\text{class}} = 1.75$ bit, so the entropy solely from quantum effects is $H(X)_{\text{quant}} = 3.25$ bit. As the quantum-mechanical process used in our scheme delivers completely symmetric results, the measured data do not exhibit any bias.

Because all noise of classical origin could in principle be known by an adversary, it must not be used to contribute to the generated randomness. Consequently, we assume the worst case, namely that these contributions carry no usable entropy. We use entropy smoothing by hashing[24,25] to eliminate these contributions, and because the amount of quantum-mechanical entropy contained in the raw data is known, we can apply a suitably chosen one-way function to project these data onto a shorter set for which the length is determined by this amount of entropy. Technically, we have performed the calculations using various cryptographic hash functions (for example, SHA512, Whirlpool, RipeMD; see refs 26 and 27) for which highly optimized implementations exist that keep pace with the physical data generation rate. The desired output bit length is achieved by hashing suitable subsets of the data, and composing the results[28].

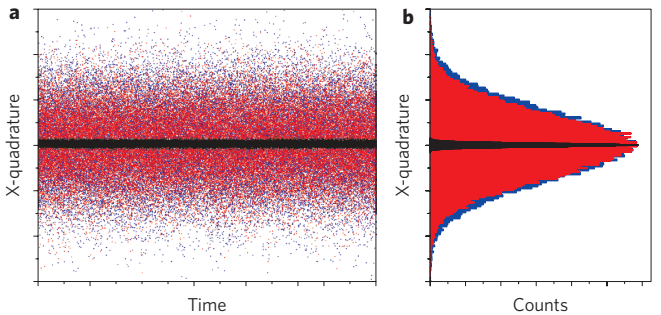

Figure 2 | Noise measurements. a, The quasi-continuous measurement outcomes of the local oscillator (blue), vacuum (red) and electronic noise (black). **b**, Resulting histograms of the LO, vacuum and electronic noise.

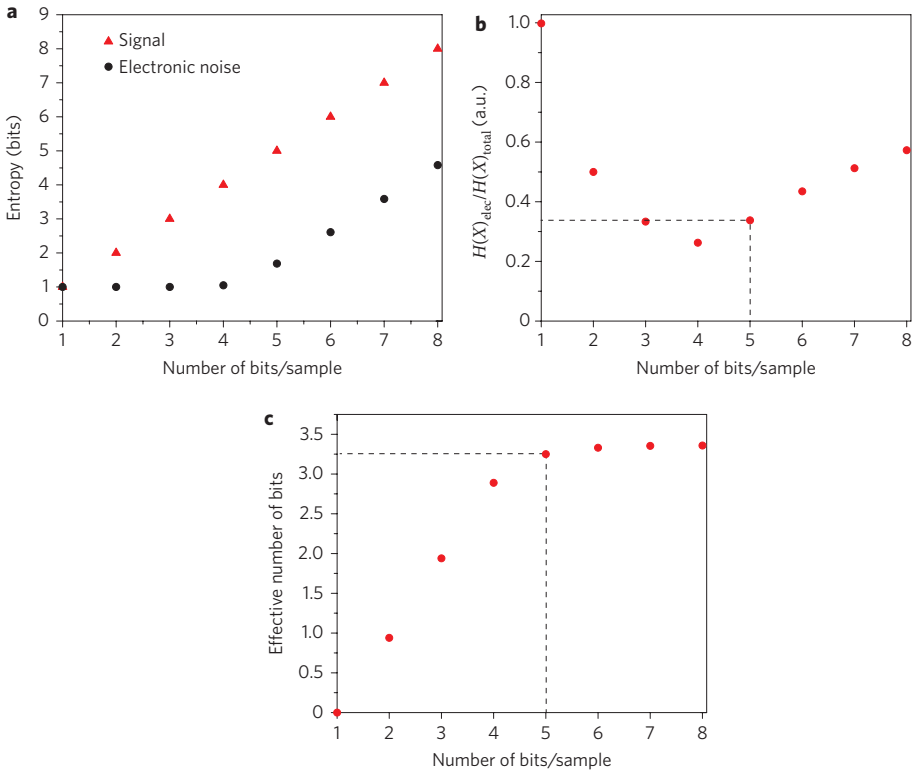

Figure 3 | Influence of classical noise on the entropy of the system. a, Entropy of the electronic signal and the vacuum state for different binnings (different number of bits per sample). **b**, Amount of entropy from electronic noise on the total entropy of the system. **c**, Effective numbers of bits achieved for different binning options.

Table 1 | Results from statistical tests to analyse randomness.

Test	Hashed variants tests passed	Raw data tests passed	Test	Hashed variants tests passed	Raw data tests passed
SerialOver	2/2	1/2	SumCollector	1/1	0/1
CollisonOver	8/8	8/8	MatrixRank	6/6	6/6
BirthdaySpacings	7/7	7/7	Savir2	1/1	0/1
ClosePairs	19/19	18/19	GCD	2/2	0/2
SimpPoker	4/4	0/4	RandomWalk	30/30	12/30
CouponCollector	4/4	0/4	LinearComp	4/4	3/4
Run of U01	2/2	0/2	LempelZiv	1/1	0/1
Permutation	2/2	1/2	Fourier3	2/2	0/2
CollisionPermut	2/2	1/2	LongestHeadRun	4/4	3/4
MaxOft	8/8	0/8	PeriodsIn Strings	2/2	0/2
SampleProd	2/2	0/2	HammingWeight2	2/2	1/2
SampleMean	1/1	0/1	HammingCorr	2/2	0/2
SampleCorr	1/1	0/1	HammingIndep	6/6	1/6
AppearanceSpacings	2/2	0/2	Run of Bits	4/4	1/4
WeightDistrib	4/4	0/4	AutoCor	3/3	1/3

The table depicts the results of the stringent *Crush* test battery of the TestU01 test suite[20]. Each test consists of several variants with different parameters. The number of tested samples in each case is so large ($\sim 3 \times 10^{10}$ bits) that the *P*-values for decisively failing tests converge to (0) or (1). The numbers of passed tests of the total number of test variants are displayed. Green numbers indicate that all test variants have been passed, whereas red numbers indicate that at least one of the test variants has been failed.

There are numerous methods that can be applied to investigate the quality of the statistical randomness of bit sequences. Most reasonable (quasi) RNGs pass most standard tests[16–19]. However, the tests of the comprehensive state-of-the-art TestU1[20] place much more stringent requirements on the data. The *Crush* test battery includes 30 tests in 139 variations. The results for our bit sequences are shown in Table 1; here the SHA512 hash-function has been used to eliminate classical noise. Although the raw data, which still contain electronic noise, fail 54% (75 of 139) of the tests, the hashed data, where these contributions are eliminated, pass all tests. Consequently, we are assured that the produced bit sequences display excellent statistical randomness. The considerable improvement of the tests when applied to the hashed data emphasizes the need to properly account for the influence of electronic noise.

With the current setup, speeds of $\sim$6.5 Mbit s^{-1} of true and unique random number generation have been achieved. To obtain higher count rates, detectors with greater bandwidths and a good signal-to-noise ratio are required. With a large signal-to-noise ratio the influence of classical noise on the measurement data is very small, which in turn leads to little hashing and therefore high generation speeds. A detector for the generation of more than

200 Mbit s^{-1} is possible with current technology and is under development.

In conclusion, a generator based on the measurement of pure quantum states to produce true and unique random numbers has been demonstrated. By measuring a vacuum state with a simple homodyne detector, the purity of the state is guaranteed. Furthermore, appropriate hashing functions are applied to eliminate all information content stemming from classical noise to ensure that the produced numbers originate only from quantum-mechanical measurement processes. By using the optimized information capacity of the continuous-variable quantum states, the speed of the system is maximized.

Methods

Measurement process. A beam of wavelength $\lambda = 1{,}500$ nm arising from a distributed-feedback laser (model SLT5411, Sumitomo Electronic Industries) was used as a LO in the homodyne setup. For convenience, the beamsplitter was replaced by a combination of a half-wave plate and a polarizing beamsplitter (PBS) to easily realize a $50/50 \pm 0.1\%$ beamsplitting ratio. The LO was incident on one port of the beamsplitter, while the second port was blocked to ensure that only a vacuum state could enter. The two emerging beams, of equal intensity, impinged on two balanced detectors. The two photocurrents of the detectors could be either added or subtracted. Both signals scaled with the amplitude of the LO and either the noise of the LO or the vacuum state.

The a.c. signals from both detectors were down-mixed using a single sinusoidal 10.5 MHz signal. The signal was amplified and then measured with a sampling rate of 2 Msamples (MS) s^{-1} on a computer using a 16-bit analog-to-digital (AD) card (Gage, CompuScope 1610-1M). The difference and sum signals were computed in post-processing. The noise arising from the difference signal was used to create the random numbers. To ensure that the electronic noise did not increase during the measurement process, it can be checked periodically. It can therefore be arranged such that the signal-to-noise ratio always exceeds a lower bound.

Furthermore, to guarantee a stable and secure system it must be verified that the common-mode rejection ratio (CMRR) of the two balanced detectors is much larger than the excess noise of the LO, otherwise this classical noise will bias the measurement outcomes. In the performed measurements the CMRR was always observed to be larger than 35 dB at a bandwidth of 1 MHz, and the LO excess noise was always smaller than 2 dB.

Binning. To extract bit sequences a binning was applied to a probability distribution derived from 499,968 sample points. As we measured a vacuum state, the mean value of the distribution was always 0. The simplest binning type is to split the distribution into two bins. All the sample points less than 0 are assigned a bit value of '1', while sample points greater than 0 are assigned a bit value of '0'. Of course, this method can be improved by binning the probability distribution into 2^n equal parts, where n is the bit combination length one wants to assign to each sample point. Here it is important to note that each bin needs to contain the same amount of samples. For example, if one has four bins, one would assign all sample points in the first, second, third and fourth bins the bit combination '00', '10', '01' and '11', respectively. This can be continued for larger values of n in a similar fashion. Furthermore, it should be noted that there are nearly no biasing effects due to the AD card. By applying the advanced multilevel strategy[29] process, which guarantees to extract the optimal number of identically distributed random unbiased bits by sacrificing bits from a biased source, this delivers only a size difference of 0.074% between the lengths of the original and processed bit streams.

Entropy calculations. The entropy containing only information from quantum-mechanical effects is given by $H(X)_{\text{quant}} = H(X)_{\text{total}} - H(X)_{\text{class}}$. The total entropy of the system $H(X)_{\text{total}}$ is given by the amount of binning as $H(X)_{\text{total}} = -\sum_{i=1}^{l+1} p_i^{\text{vac}} \log_2 p_i^{\text{vac}}$, where p_i^{vac} is the probability to find a measurement outcome in the ith bin of the $l+1$ bins of the probability distribution of the vacuum state. As a result of our binning method, $H(X)_{\text{total}} \cong \log_2(l+1) = n$, where n is the length of the bit combination assigned to each sample point. The entropy of all classical effects is given by $H(X)_{\text{class}} = H(X)_{\text{elec}} + H(X)_{\text{balan}}$, where the entropy of the electronic noise $H(X)_{\text{elec}} = -\sum_{i=1}^{l+1} p_i^{\text{elec}} \log_2 p_i^{\text{elec}}$ contributes most. Here p_i^{elec} is the probability to find a measurement outcome of the electronic noise again in the ith bin of the vacuum state. The entropy of the electronic noise is estimated by centring the histogram of the electronic noise data inside the signal's histogram as shown in Fig. 2. Subsequently, the binning for the signal is also applied to the electronic noise. Because in the centre the bins have the smallest width, an upper bound for the entropy value of the electronic noise is determined. Furthermore, it should be noted that the better the signal-to-noise ratio, the smaller the entropy of the electronic noise. In our measurements, a minimum signal-to-noise ratio of 25 dB is guaranteed by constantly monitoring the power of the LO. The entropy of LO noise due to imperfect balancing, $H(X)_{\text{balan}}$, only has a comparably small impact. It can be determined by knowing the maximum possible asymmetry of the beamsplitter and treating all noise coming from the LO as classical noise. This way an upper bound for $H(X)_{\text{balan}}$ can be set, which in our case is $H(X)_{\text{balan}} = 0.06$ bit.

Hashing and statistical tests. The stringent *Crush* test of the TestU01 test suite[20] was applied to both the raw and hashed data (see Table 1). Although the raw data (which still includes electronic noise) fail numerous tests, the hashed variants exhibit no weaknesses. Similarly successful results are only obtained with the best currently known random number generators (see Table 1 in ref. 20). Notice that we have also successfully performed tests with the DieHard and FIPS statistical test batteries, the results of which are not shown.

The results presented here are obtained by using the SHA512 hash-function. A difference in entropy between the different hash-functions has not been observed. The randomness of our obtained numbers is guaranteed to originate from quantum noise solely, as the output of a hash-function applied to an input with sufficiently high entropy is arbitrarily close to uniform randomness, even for quantum-mechanical side information[30]. Furthermore, we would like to emphasize that field-programmable gate array (FPGA) implementations exist for the current hash-functions, so integration to any standard computer system is easily achievable.

Received 24 November 2009; accepted 13 June 2010; published online 29 August 2010

References

1. Metropolis, N. & Ulam, S. The Monte Carlo method. *J. Am. Statist. Assoc.* **44,** 335–341 (1949).
2. Schindler, W. *Cryptographic Engineering* Ch. 2 (Springer Science + Business Media, 2009).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Modern Phys.* **74,** 145–195 (2002).
4. Walker, J. HotBits: genuine random numbers. http://www.fourmilab.ch/hotbits/.
5. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71,** 1675–1680 (2000).
6. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **47,** 595–598 (2000).
7. Bronner, P., Strunz, A., Silberhorn, C. & Meyn, J. P. Demonstrating quantum random with single photons. *Eur. J. Phys.* **30,** 1189–1200 (2009).
8. Kwon, O., Cho, Y.-W. & Kim, Y.-H. Quantum random number generator using photon-number path entanglement. *Appl. Opt.* **48,** 1774–1778 (2009).
9. 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).
10. Stipcevic, M. & Rogina, B. M. Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum.* **78,** 045104 (2007).
11. Trifonov, A. & Vig, H. Quantum noise random number generator. US patent 7,284,024 (2007).
12. Fiorentino, M., Santori, C., Spillane, S. M., Beausoleil, R. G. & Munro, W. J. Secure self-calibrating quantum random-bit generator. *Phys. Rev. A* **75,** 032334 (2007).
13. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021–1024 (2010).
14. Svozil, K. Three criteria for quantum random-number generators based on beam splitters. *Phys. Rev. A* **79,** 054306 (2009).
15. Sych, D. & Leuchs, G. Quantum uniqueness. Preprint at arXiv:1003.1402 (2010).
16. Marsaglia, G. Diehard: a battery of tests of randomness. http://www.stat.fsu.edu/pub/diehard/.
17. Brown, R. Dieharder. http://www.phy.duke.edu/~rgb/General/dieharder.php.
18. Walker, J. ENT test suite. http://www.fourmilab.ch/random/.
19. Rukhin, A. *et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology, Special Publication 800–22 (NIST, 2001).
20. L'Ecuyer, P. & Simard, R. TestU01: A C library for empirical testing of random number generators. *ACM Trans. Math. Softw.* **33,** 22 (2007).
21. Uchida, A. *et al.* Fast physical random bit generation with chaotic semiconductor lasers. *Nature Photon* **2,** 728–732 (2008).
22. Agnew, G. B. *Advances in Cryptology—EUROCRYPT'87*, 77–81 (Springer Verlag, 1988).
23. Wallace, C. S. Physically random generator. *Comput. Syst. Sci. Eng.* **5,** 82–88 (1990).
24. Impagliazzo, R. & Luby, M. One-way functions are essential for complexity based cryptography. In *30th FOCS*, 230–235 (IEEE Computer Society, 1989).
25. Cachin, C. Hashing a source with an unknown probability distribution. *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, 1998).

26. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (John Wiley & Sons, 1996).
27. Barreto, P. S. L. M. & Rijmen, V. The whirlpool hashing function. http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html (2010).
28. Stinson, D. R. Universal hashing and authentication codes. *Designs, Codes and Cryptography* **4,** 369–380 (1994).
29. Peres, Y. Iterating von Neumann's procedure for extracting random bits. *Ann. Stat.* **20,** 590–597 (1992).
30. Tomamichel, M., Schaffter, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. Preprint at arXiv:1002.2436 (2010).

Acknowledgements

This work was supported by the EU project Q-ESSENCE and the Danish Research Council.

Author contributions

U.L.A. conceived the original concept and proposed the experiment. Experimental work and some of the data analysis were carried out by C.G. together with C.W. and R.D.. W.M. conducted the theoretical investigations on the hashing and statistical tests as well as the final data analysis. D.S. contributed to theoretical investigations and proposed the idea of unique random numbers. Project planning was carried out by C.W., U.L.A., D.S., C.M. and C.G.. The paper was written by C.G., C.W., W.M., C.M., D.S., U.L.A. and G.L.. The project was initiated and supervised by U.L.A., C.M. and G.L.

Additional information

The authors declare no competing financial interests. Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/. Correspondence and requests for materials should be addressed to C.G.