SCIENTIFIC REPORTS
natureresearch

OPEN

Single Photon Randomness based on a Defect Center in Diamond

Xing Chen[1], Johannes N. Greiner[1], Jörg Wrachtrup[1,2] & Ilja Gerhardt[1]*

The prototype of a quantum random number generator is a single photon which impinges onto a beam splitter and is then detected by single photon detectors at one of the two output paths. Prior to detection, the photon is in a quantum mechanical superposition state of the two possible outcomes with –ideally– equal amplitudes until its position is determined by measurement. When the two output modes are observed by a single photon detector, the generated clicks can be interpreted as ones and zeros – and a raw random bit stream is obtained. Here we implement such a random bit generator based on single photons from a defect center in diamond. We investigate the single photon emission of the defect center by an anti-bunching measurement. This certifies the "quantumness" of the supplied photonic input state, while the random "decision" is still based on the vacuum fluctuations at the open port of the beam-splitter. Technical limitations, such as intensity fluctuations, mechanical drift, and bias are discussed. A number of ways to suppress such unwanted effects, and an a priori entropy estimation are presented. The single photon nature allows for a characterization of the non-classicality of the source, and allows to determine a background fraction. Due to the NV-center's superior stability and optical properties, we can operate the generator under ambient conditions around the clock. We present a true 24/7 operation of the implemented random bit generator.

The generation of random bits is a growing field of quantum science. A primary quantum process and a subsequent measurement allow to implement an inherently unpredictable measurement outcome. In this sense a quantum randomness generator follows Born's rule, which describes the measurement outcome of a quantum measurement as fundamentally probabilistic. Further, the interest in quantum random numbers is testified by the fact that the most popular available products in quantum technology are quantum random number generators. Some companies are selling quantum random number generators, which emit a stream of ones and zeros, supposed to fulfill the crucial requirements of a random number: The number of ones and zeros is approximately equal, and no memory and no correlation among two or more bit outcomes is evident – the numbers are *independent and identically distributed*. Most commonly a user has problems to verify that the emitted stream is based on a true quantum process and not deterministically pre-programmed or at least predictable by an evil manufacturer or other adversary. The latter would be feasible since a recent discussion in cryptography identified the supply of *weak* random numbers as a reasonable attack vector of modern cryptography[1,2]. Such *kleptographic* attacks[3] pose an important threat to modern information security technology. Therefore the question exists how such devices might allow a user to examine and to ensure the integrity of a primary random process and follow the randomness processing.

Apart from early, mostly theoretical descriptions[4–6], a variety of quantum random number generators were implemented around the turn of the century[7,8]. These early generators were based on the measurement of photonic qubits. With the increasing demand of speed and the implementation of coherent states, a number of generators were implemented which use other light sources than single photons. These generators often measure the vacuum fluctuations[9–11] or phase noise[12,13]. In the past years the implementation of device independent randomness generators[14,15] or self-testing schemes[16] has been experimentally demonstrated. A timely review has been written[17].

Although a single photon which impinges on a beam splitter and is later detected is still the most prominent model system for a quantum decision, only very few implementations of true *single* photon randomness have been demonstrated – mostly due to the implied technical complications and the questionable benefit of such an implementation. The few experiments introduce single photons from a down-conversion source which impinge on a beam splitter[18,19], or on an integrated optics device[20].

[1]3rd Institute of Physics, University of Stuttgart and Institute for Quantum Science and Technology (IQST), Pfaffenwaldring 57, D-70569, Stuttgart, Germany. [2]Max Planck Institute for Solid State Research, Heisenbergstraße 1, D-70569, Stuttgart, Germany. *email: i.gerhardt@pi3.uni-stuttgart.de

As for single photon sources, a large variety of single emitters as single photon sources has been investigated in the past. One prominent example is the negatively charged nitrogen-vacancy center. It has been experimentally singled out since 1997[21]. Besides its properties as nanoscopic sensor and tool for spin based quantum information processing, it represents a stable single photon source with up to few million counts per second[22–24]. A variety of single photon based implementations were realized based on defect centers in diamond, for example quantum cryptography[25], or other fundamental experiments[26]. Only few experiments were performed which utilize the single photon emission of a NV-center for quantum randomness generation. Only recently a single NV-center in a sample was utilized for quantum randomness generation based on the polarization detection of a single photon[27].

Here we theoretically discuss and experimentally implement a single photon based quantum random number generator. The single photon stream originates from a single nitrogen-vacancy-center in diamond. The device is operated for more than a week in continuous operation. The entropy of the raw bit stream is estimated with a conservative a priori model. The single photon nature allows for a characterization of the non-classicality of the source, but yields naturally a lower randomness rate than generators, which rely on the detection laser noise or laser phase fluctuations[13]. Furthermore the amount of unwanted, technical background clicks can be estimated by this model. In how far this leads to a certifiable randomness generation is discussed. The advantage of a true single photon source allows a user to exclude a number of attack scenarios and to guarantee to a certain extend the independence to an external adversary of the device.

Theory

Under discussion is a random bit generator, in which the outcomes on two discrete single photon detectors in different output modes of a beam-splitter are interpreted as single raw bits. This section describes the fundamental ideas to process the raw detector outcomes, i.e. the electrical "clicks" of the two detectors. These bits then go into some post-processing, namely a randomness extraction process. For the calculation of the underlying entropy, the outcome probabilities and the transition probabilities are relevant. These single and transition probabilities are calculated in full in the supplementary material. In total three models are introduced, which describe increasingly more conservative interpretations of the raw-bits.

Single photon stream. A stream of single photons is guided in a spatially single optical mode towards a beam-splitter. The second input arm of this beam-splitter is blocked, which is commonly described as a vacuum state ($|0\rangle$) in the second input arm. Therefore, the single photons probability amplitudes are distributed on the beam-splitter according to the beam-splitter ratio. The photons are subsequently detected on the detectors A (transmitted photons) and B (reflected photons).

For the first model, we simply consider *all* generated clicks as raw random bits. The probability of the individual outcomes and the transition probabilities are relevant. Here we discuss the fundamental parameters to estimate the entropy in the next section. Our interpretation is not limited to the use of a single photon input state, but it might still be advantageous due to an increased click rate on a single photon detector by the interplay of detector dead times and the characteristic time constant of a single emitter[28].

The probability whether a photon is detected in one or the other output path is fundamentally linked to the presence of the vacuum state at the second input port of the utilized beam-splitter. Further, it is dependent on a variety of experimental factors. Most importantly, the beam splitter ratio $\mathscr{R}$ is a function of the reflection (R) and transmission (T) coefficient. For simplicity, a loss-less beam-splitter is assumed, i.e. $T + R = 1$. This does not imply an equality of the two coefficients, i.e. the beam-splitter can still be biased. Although a biased beam splitter does introduce some imbalance, it does not necessarily introduce any memory in the system, and can therefore represent a perfect Bernoulli trial with a given probability distribution.

Another crucial parameter in the (im-)balance of the detector recordings is the detector efficiency of the utilized detectors, $\eta_{\{A,B\}}$. This value describes how many of the incident photons actually lead to an electrical pulse which can then be recorded. In a given experimental implementation, the individual detector efficiency is closely linked to the beam-splitter ratio. Both factors can not be independently measured in a simple way in a given setting.

An electrical pulse from a single photon detector has to have a finite length, such that it can be recorded with normal detection hardware. During this time, a second detection event is usually suppressed. This time of suppression is called the "dead-time", τ_{dead}, of the detector. In the common Geiger mode photo detector modules the time where no second photon is detected, commonly exceeds the length of the electrical pulse. This dead-time can be described by a correction factor, which relates the click rate to the actual single photon flux onto the detector. At low incident photon counts and low dark-counts of the detector, the factor is close to unity. This factor accounts for the undetected photon events, which are suppressed as a second event which should have been launched although the detector was still found within its dead-time.

The technicality of the detector dead times also introduces another problem for the generation of random bits: Two subsequent clicks on different detectors can be dependent, since one of the detector is in its dead time, only the other detector is capable of detecting another photon. In the limiting case for very high count-rates this leads to an alternating bit pattern with zero entropy, because when the detector is able to detect a next photon, it immediately receives one and generates another click. This leads to an anti-correlation of detector events, and becomes dominant at higher count rates where the probability of coincidental clicks is non-zero[28].

Subsequently, the total click rate on the detectors is $r_{\mathrm{total}} = r_{\mathrm{A}} + r_{\mathrm{B}}$. It amounts to the following expression. To recall: the behavior between generated raw bits and the incident intensity is not strictly linear.

$$r_{\mathrm{A,B}} = \eta_{\mathrm{A,B}} T I_{\mathrm{in}} - \frac{(\eta_{\mathrm{A,B}} T I_{\mathrm{in}})^2 \int_0^{\tau_{\mathrm{dead}}^{\mathrm{A,B}}} g^{(2)}(\tau) d\tau}{4} \tag{1}$$

where $\eta_{\mathrm{A,B}} T I_{\mathrm{in}}$ is the click rate when no dead-time would be present, and $g^{(2)}(\tau)$ is the anti-bunching curve[29] of the utilized single photon source.

This equation accounts for the click rates independently of the input light source. A laser source obeys an exponential decaying probability distribution in the subsequent detection of a photon. At the same incident photon flux, a single photon source has a higher probability of a later detection event and might generate a larger randomness generation rate than a laser with the same brightness. This relates to an interplay of the detector's dead-time and the count rates. More details are outlined in[28].

The detection rates for the two utilized detectors have been determined by the consideration of the beam splitter ratio, the individual detection efficiency and the individual dead times. The *probabilities* for calculating the entropy below can be experimentally determined straight forwardly by the ratio of the detector events:

$$p_{\mathrm{A}} = \frac{r_{\mathrm{A}}}{r_{\mathrm{A}} + r_{\mathrm{B}}}. \tag{2}$$

The conditional probabilities are correspondingly calculated as follows. Here we exemplary show the derivation for the case of the conditional detection of $p(A|A)$:

$$p(A|A) = \left(1 - \int_0^{\tau_{\mathrm{dead}}^{\mathrm{A}}} g^{(2)}(\tau) d\tau\right)\eta_{\mathrm{A}} T \tag{3}$$

This is outlined in the supplementary material in more detail. The deviation of the conditional probabilities from the ideal value of 0.5 is dominated by the combination of the detector efficiencies and the beam-splitter ratio. The specific detector dead times influence the conditional probabilities of the conditional photon detection events only at increased count rates.

In this section we have considered that *all* generated photon detection events act as a source of raw quantum randomness. The underlying entropy relates to the bias and other technical consideration such as the detector efficiency and the dead-time of the detectors. The calculated probabilities and the conditional probabilities are utilized to calculate the min-entropy below.

Bounds on quantumness. The above description of photon click rates is applicable correspondingly to a simple laser or a light-emitting diode (LED) input source. Equivalently, we would effectively sample the vacuum fluctuations which determine the output of the measurement at the beam-splitter. On the other hand, the use of a laser has some drawbacks: When a coherent state, $|\alpha\rangle$, is present, the user has no indication if the device *really* detects the incoming (laser) mode. A counter example could be that the device was misaligned in the past and only uncorrelated photons from two independent sources are detected. The two beams which impinge from a laser via the beam-splitter onto the detectors are unrelated in a number of ways, and cannot be differentiated if two different lasers (or two independent laser modes) were observed with the detectors. In the worst case, an eavesdropper will remote-control the detector clicks and due to their initially uncorrelated origin, the owner of the device will have no proof on their origin or integrity.

Therefore, another strategy of an eavesdropper could be to simply send uncorrelated counts into the two detectors. In the case of the laser source, this flaw would not be indicated by any measurable quantity, except that possibly more counts per unit time are present.

A single photon source is of advantage at this point and might lead to some enhancement of the trust in the random bit generation scheme. As an ultimate proof to have a single photon emitter, an auto-correlation function can be recorded. For a single photon source, this shows the typical single photon anti-bunching. This gives an upper bound on how much randomness can be extracted, when we assume that the random bit generator is equipped with a single photon emitter. The amount of (uncorrelated) counts, which might be remotely controlled events, can be well determined. Furthermore, a certain guarantee is given, that one single mode is detected and the detector does not observe e.g. uncorrelated sources.

Naturally, for a single photon input state, the photons arrive at the beam-splitter in an *anti-bunched* fashion. This implies, that after a photon detection event on one detector, the second detector does not observe a single click within a characteristic time.

Anti-bunching is commonly described by the auto-correlation function $g^{(2)}(\tau)$. In an ideal case $g^{(2)}$ for zero time delay ($\tau = 0$) amounts to zero, and at a photon detection event no other detection is observed. In this case, all the detected raw bits are originating from a fundamental quantum process, and we consider all raw bits as quantum random bits. In reality, a recording of $g^{(2)}(0) = 0$ is very hard to achieve: The dark counts of the detectors, any kind of background contributions from the environment, and also the electrical jitter of the experimental devices, are factors which will be mixed with the single photon events and increase the final value of $g^{(2)}(0)$. Since all these spurious background contributions introduce uncorrelated events, we consider such events as being based on clicks which can be known to an external adversary called "Eve". Subsequently, this fraction of uncorrelated events is discarded by a later randomness extraction process.

The term *true single photons* denotes all the photons which are detected by the detectors and stem from the device-internal single photon source. Usually, measurement artefacts reduce this fraction from unity. Still this fraction can be well determined by the so-called anti-bunching curve, as $\sqrt{1 - g^{(2)}(0)}$. The anti-bunching characterizes the quantum nature of the involved photons, and it cannot be interpreted by classical theory[29]. Subsequently, the single photons which are characterized by anti-bunching are generated by a fundamental quantum process, while their distribution over the detectors (still) relies on the vacuum fluctuations on the beam splitter.

Also, the recording of the anti-bunching curve allows to estimate a background fraction. This is performed by analyzing the correlation function at zero time delay. This allows to give an estimation on the "quantumness" of the single photon stream. While in the model above *all* photons were considered, we now bind the amount of randomness generation clicks on the amount of true single photons in the stream. This requires the assumption, that the randomness generator contains a single photon source and that the underlying randomness is bound on the vacuum state on the second input port of the beam splitter.

In order to estimate the amount of click events which are generated by a quantum process, the fraction of single photon events in the entire photon stream is determined. The fraction of single photon events is known as $\sqrt{1-g^{(2)}(0)}$ [23], where the non-zero value of $g^{(2)}(0)$ testifies a background fraction. Subsequently, all the generated raw-clicks can be reduced by hashing down to the conservative bound of the below calculated entropy. When $g^{(2)}(0) \geq 1$, all the raw random data will be discarded. In this case, the source for the generator is no longer based on the device internal single photon source[29,30], and the bit generation process is likely to be externally influenced and in the worst case completely controlled by Eve.

For the calculation of the probabilities, we refer to the discussion above. The consideration of background events implies that a few of the generated bits are actually known to an eavesdropper. Therefore it is not clear if they were generated by the genuine device, or if they were introduced in an uncorrelated manner. This fraction is accounted for in the supplementary material by introducing a probability, that the eavesdropper is aware of the generated bit, p_e. This discussion extends also to the derivation of the conditional probabilities, which are required to estimate the min-entropy of the generator under these considerations.

Conditioned tuple detection of detector clicks. As outlined above, every recording of anti-bunched light is subject to background influences. This usually originates from the sample under study or external sources such as ambient light. In the worst case –especially under conservative considerations– this might also originate from an external adversary, who controls the detectors in an uncorrelated fashion. Therefore, all considerations on the entropy of this single photon stream were bound to the amount of "true" single photons, which can be estimated by the recording of anti-bunching. Such a recording exhibits a small fraction of photons, which are time-wise anti-correlated – the anti-bunching dip. On the other hand, an auto-correlation function around $g^{(2)}(\tau) = 1$ implies that the photonic emitter has no memory, and no photon-photon correlation, for a particular waiting time τ. This is given for photon detection events which are time-wise separated, and do not have a "partner-photon" which can be used to characterize the (anti-)correlation. Above we have assumed, that the recording of anti-bunching describes the *full* data stream, even if a photon was detected with no further closely neighboring detection events, which would then have been suppressed and would directly testify the anti-bunching.

This assumption is based on the idea that the photonic stream is fair sampled. This means that the photons which are not contributing to the small time-window of the anti-bunching dip (approx. 1–30 ns, corresponding to the T_1-time of the system) are assumed to be still genuine single photons. Of course, statistical evidence allows us to consider this assumption is proven. Ideally, a normalized anti-bunching dip is below unity, but some parameters of the experimental devices may have fluctuations, and may cause that the anti-bunching exceeds the value of unity. To guarantee the quantumness of the extracted bits from the raw data, we now only consider the data in a time window below the line of unity (classical line). By considering the fluctuation of the single photon events, we limit the area of random bits to the area which is clearly below this classical boundary. This implies a time-wise selection to events which have a "partner-photon" temporally close-by.

As for the recording of the anti-bunching curve, only the *tuples* of photon detection events are considered. These are events which are often described as "start-stop events" on two photon detectors behind a beam splitter. Fundamentally, these tuples are balanced, since the probability of detecting the bit pair "AB" and "BA" depends on the individual probabilities of detecting photons and the corresponding pair-detection probabilities are equal $p(\mathrm{AB}) = p(\mathrm{BA})$, as long as the experimental parameters do not change in the course of the experiment. While this tuple detection scheme introduces an advantage due to its inherently balanced nature, it also reduces drastically the detection rate of the raw randomness events, since only start-stop events in a limited time range are utilized. This start-stop event detection scales approximately quadratically (more insights below) with the single count-rates and is usually orders of magnitude smaller than in the simple methods which are described above.

For the selection of anti-bunched detection tuples, we only select the bits which are clearly below a level of $g^{(2)}(\tau) = 1$. These events are clearly anti-correlated, but are still above the background level in the $g^{(2)}(\tau)$-recording. In this area below the anti-bunching curve, we consider the pair "AB" as one random bit, "BA" as the other random bit (Note here that we are dealing with binary random bits, so we only have two random bits: 0 or 1). These are events, where one detector clicked, while the other one had just fired. This implies that these newly defined raw bits are bound to a detection of a pair of photons in both arms.

Ideally, a normalized anti-bunching curve of an ideal two-level system exists only below unity. This implies, that the considered values *all* fulfill the non-classical nature of $g^{(2)}(\tau) < 1$. In a real-world scenario, some parameters of the experimental devices may have fluctuations. These may be introduced as shot noise. To guarantee the quantum nature of the utilized light source, in this situation, we consider the data below unity with given standard deviations, for example, 11.5σ deviations, which limits the probability of an outlier significantly.

An external adversary has now limited options to influence the device based on the strategy of tuple detection: Any uncorrelated event which is controlled from an external entity will lead to an increased background fraction. This would also be suppressed by the prior method on limiting the amount of randomness to the single photon nature of the entire stream and discarding the background. Therefore, an external adversary would have to implement more subtle strategies to launch clicks in the generator.

A more subtle strategy could be, that when a click is launched by the primary process, i.e. an emitted photon from the single photon source, Eve has to quickly launch a click onto the other detector of the generator – simply since the first detector will be in its dead time. As discussed below, this requires a stringent timing of the clicks launched by Eve. First, Eve has to *detect* that there has been a click in the generator; then she has to *introduce another click* into the generator. If the legitimate time frame is very short, Eve has to be very close to the generator – simply due to the signal traveling time. Obviously, if Eve is outside the light cone, she has no option to launch clicks and to influence the generator at her will. In this sense, the generated bits which are based on short time differences (−ns) in subsequent clicks in the generator are "fresh" and guaranteed to be unaltered for a short amount of time.

Another, more sophisticated attack version of Eve can be to fake the clicks on both detectors, as if Eve had another single photon source at her location. Then, the number of clicks, which are outside the small nanosecond range of the primary source is large. Depending on the relative brightness compared to the primary source this will lead to a certain amount of background clicks again. The only option that Eve has, is to fully suppress the primary emission of the single photon source and replay an equivalent detector control scheme which would introduce a comparable anti-bunching signal. A simple control of the primary photon source by another method can reveal that an external adversary is active.

To calculate the probabilities for the next entropy extraction step, the start-stop event (tuple) probabilities $p(AB)$ and $p(BA)$ are considered. Furthermore, the conditional probabilities (e.g. $p(AB|AB)$) have to be described. For a full derivation see the supplementary material.

A Priori Entropy Analysis and Randomness Extraction

We now turn to the amount of extractable entropy for the generator. This is the key measure for any randomness generator and allows to post-process the raw input bits. Naturally every generator has to perform some post processing, since the true amount of randomness in any experimental configuration can only be determined to a certain level of accuracy. Then one has to consider, that even a sophisticated characterization run is just an accidental outcome. Subsequently, we have to consider a conservative bound, which allows to reduce the number of bits to the true entropy fraction which is available from the raw random stream. This reduces the amount of bits which are extracted from the raw bits.

For all the three discussed cases above, we need to estimate the conditional min-entropy for post-processing the random bits. The definition of the required conditional min-entropy, H_∞ is given as[28,31]:

$$H_\infty(X|Y) = -\log_2\left(\sum_y p(y)\max_x\{p(x|y)\}\right), \tag{4}$$

where x and y are the subsequent events of random bits. In this definition the single and the transition probabilities are the crucial parameters, and they can all be derived from the experimental parameters as discussed above.

For the first case described above, we want to use two universal hashing as an extractor to generate a nearly uniformly distributed random string[32]. In the generated raw random bits, the number of zeros and ones are not always the same. Different parameters may influence this bias between zeros and ones. For the security of the random bits, the conditional min-entropy is calculated. The conditional min-entropy is defined as before (Eq. 4).

The conditional min-entropy is a more strict bound than conditional Shannon entropy. With the theoretically estimated bound of $H_\infty(X|Y)$, randomness extraction could be applied to achieve a nearly uniformly distributed random string. To be specific, from the experimental parameters, the value of $H_\infty(X|Y)$ could be derived by the relevant probabilities, suppose $H_\infty(X|Y) = k$, then for the n bits long raw random data, approximately kn bits nearly uniform distributed random data could be extracted. The generation speed of the raw bits is r_{total}, then the generation speed of the unbiased random bits amounts accordingly to kr_{total}.

For the second case, only the single photon fraction of the assumed fair sampled stream is considered. We now estimate the min-entropy of the stream under consideration of the background fraction. This requires that our model is extended with a third possible outcome, which is associated to an eavesdropper or classical background light. The outcomes would therefore be A, B and the events known to an eavesdropper E. The probabilities are not only considered as genuine outcomes of the two detectors, but a third probability is introduced, which denotes that the generator's outcome was not generated by the given single photon source, but by Eve. This fraction reduces the overall amount of entropy of the generator. The probability of a *known* outcome, which is generated by Eve, is a function of the observed $g^{(2)}_{\text{fit}}(0)$, which indicates any deviation to a true single photon stream.

As shown in the Supplementary Material, the fraction of pure single photon events is $\sqrt{1 - g^{(2)}_{\text{fit}}(0)}$. The probability of having an event from the eavesdropper relates accordingly to the $g^{(2)}$-function: $p_e = 1 - \sqrt{1 - g^{(2)}_{\text{fit}}(0)}$. This fraction of non-single photon events may also change the conditional probability of $p(x|y)$.

Now, all input parameters for the generator are defined. We discard probabilities in our consideration which could be known by an eavesdropper. Also events, which are influenced by an eavesdropper are neglected. This reduces the equation to:

$$H_\infty(X|Y) = -\log_2\left(p_e + (1 - p_e)\left(\sum_y p(y)\max_x\{p(x|y)\}\right)\right). \tag{5}$$

Compared to the above Eq. (4), the extractable entropy given by the Eq. (5) is reduced. However, the random bits which can be extracted by this equation are generated by single photon events, which means they are considered to originate from the genuine source of the generator. Suppose $H_\infty(X|Y) = k_{\text{q}}$ in this case, then with an n bits long raw data stream, accordingly $k_q n$ quantum bits could be extracted from the raw bits. The generation speed of this unbiased quantum random number corresponds to $k_q r_{\text{total}}$.

For the last case, only paired events and the *area* below unit line (i.e. $g_{\text{fit}}^{(2)}(\tau) < = 1$) are considered. This line is treated as the classical limit[29,30,33]. This area is used to determine the fraction of very conservative considered single photon quantum randomness from the raw data. In order to estimate this fraction, the click rates of the raw events are required. For the convenience of description, this area is named as the "quantum area" in the following.

The quantum randomness fraction can be derived by considering the start-stop events for a given timing resolution τ_{rs}. The start-stop event rate, r_{stsp}, of the two detectors and uncorrelated events (e.g. laser emission) is given for a certain time resolution τ_{rs} as:

$$r_{\text{stsp}} = r_{\text{A}} \times r_{\text{B}} \times \tau_{\text{rs}}.$$

We like to note the difference by a factor of two against our prior work[28], which is caused by disregarding the order of the events in this case.

In the "quantum area", at different delay times, the start-stop events in a given timing resolution, τ_{rs}, correspond to different $g^{(2)}(\tau)$ values. This means they obey different probabilities[33]. The experimental anti-bunching curve is represented as $g_{\text{fit}}^{(2)}(\tau)$. Then, the total photon start-stop event rate in this quantum area is given by

$$r_{\text{A}} \times r_{\text{B}} \times \sum_{\tau=-t}^{\tau=t} \tau_{\text{rs}} g_{\text{fit}}^{(2)}(\tau) \approx r_{\text{A}} \times r_{\text{B}} \times \int_{-t}^{t} g_{\text{fit}}^{(2)}(\tau) d\tau,$$

where t satisfies $g_{\text{fit}}^{(2)}(t) = 1$, which means that the entire range is considered until the events are not anti-correlated any more. $g_{\text{fit}}^{(2)}(\tau)$ is the anti-bunching curve with background, which means the above equation also includes the start-stop events caused (partially) by background noise. In order to deal with this situation, we use, as above, the fraction $\sqrt{1 - g_{\text{fit}}^{(2)}(0)}$ to exclude the background noise in the clicks of each detector. Then the start-stop events originating from the single photon events are

$$r_{\text{stsp}} = (1 - g_{\text{fit}}^{(2)}(0)) \times r_{\text{A}} \times r_{\text{B}} \times \int_{-t}^{t} g_{\text{fit}}^{(2)}(\tau) d\tau. \tag{6}$$

Their count rate in this area is the generation speed of single photon events which are short-time related. The tight bound of the randomness generation to the genuine source of the described generator is guaranteed by the short time distance of the start-stop events *AB* and *BA*. Therefore, the generation speed of the quantum random bits in this part is linked to the start-stop events as $r_{\text{rand}} = r_{\text{stsp}}$.

With this start-stop event count rate, the fraction of extractable quantumness per raw bit is determined.

Notice that the quantum random bits which are generated tight to this area are supposed to be well balanced. The raw bits are generated at a speed of r_{total}, so the fraction of quantum random bits from per raw bit is $r_{\text{rand}}/r_{\text{total}}$. This value is affected by the shape of the anti-bunching curve and $g_{\text{fit}}^{(2)}(0)$. An extreme case is that when the background noise dominates, such as $g_{\text{fit}}^{(2)}(0)$ is unity. In this case, we can not extract any quantum randomness from the raw bit data.

Since the fraction of quantum randomness per raw bit is $r_{\text{rand}}/r_{\text{total}}$, the rest $1 - r_{\text{rand}}/r_{\text{total}}$ bits are considered as classical noise, and, to be conservative, as to be known by Eve. Correspondingly, $p_c = 1 - r_{\text{rand}}/r_{\text{total}}$, is the fraction of classical noise in the raw random data. The conditional min-entropy in this case can be written as:

$$H_{\infty}(X|Y) = -\log_2\left(p_c + (1 - p_c)\left(\sum_{\mathbf{y}} p(\mathbf{y}) \max_{x}\{p(\mathbf{x}|\mathbf{y})\}\right)\right). \tag{7}$$

Experiment

The above discussed schemes are experimentally realized. First, the experimental configuration is discussed. After this, the experimental subtleties are characterized and the entropy is estimated for the experimental data according to the three prior discussed cases.

Experimental Implementation.

The single photon source used for randomness generation consists of the emission of a single nitrogen-vacancy center which is optically excited by a continuous wave laser. The resulting fluorescence is detected by confocal microscopy (simplified in Fig. 1a). The entire experiment is operated under ambient conditions, and spans less than 1 m^2 of an optical table.

The laser ($\lambda = 532$ nm) which is used to excite the single emitter is operated in continuous wave mode, i.e. the utilized laser is always on. To avoid laser power fluctuations, the laser intensity is stabilized by a commercial PID-controller (Stanford Research, SIM960). For this, the laser power is detected shortly before the diamond single photon source. The laser power is regulated by an acousto-optical modulator which is located at the laser output. For mode-cleaning, the laser light is then guided by an optical single-mode fiber and introduced into the microscope.

After the laser beam is reflected off a dichroic mirror it is guided to a galvanometric mirror system which steers the beam to a 4 *f*-scanning microscope. Focusing is realized by an 100× oil objective (Olympus Plan FL N, NA = 1.35). In the confocal configuration, the emitted light is then captured by the same microscope objective, guided backwards, and transmits through the dichroic mirror towards the detection system. To suppress unwanted stray light, the detected light is then tightly focused ($f = 100$ mm) onto a pinhole ($\varnothing = 50\,\mu$m) and fil-

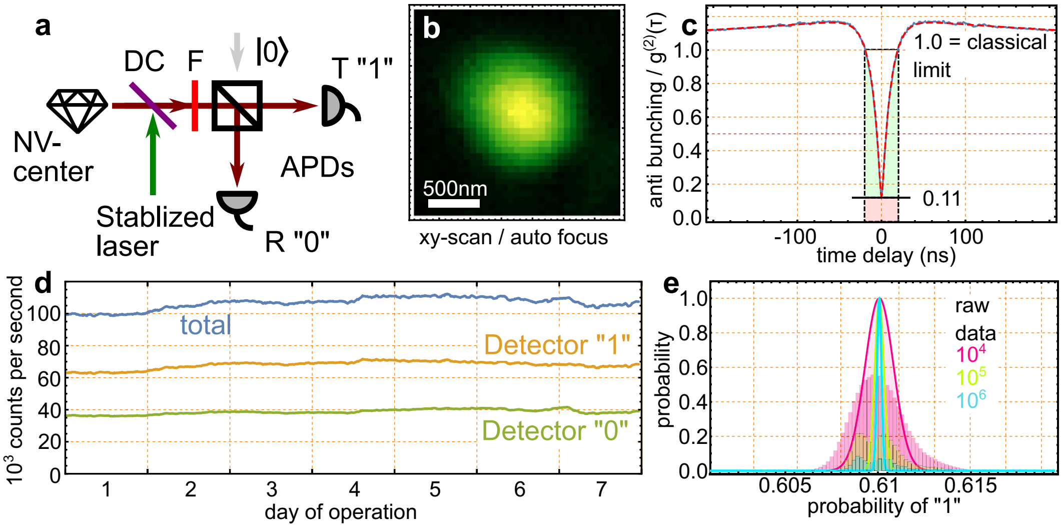

Figure 1. Experimental Configuration. (**a**) Scheme of the experimental configuration. A confocal microscope is used to observe a single nitrogen-vacancy center. The detection is performed with two avalanche photodiodes (APDs). DC = Dichroic Mirror; F = Long-pass Filter. (**b**) Fluorescence counts of a lateral scan over the sample. Peak intensity: 100 kcps (kilo counts per second). (**c**) Measurement of anti-bunching and a theoretical fit (dashed line), the timing resolution here is 0.5 ns. (**d**) A long time recording in the course of 7 days, the exact time is 608125 seconds. (**e**) Presentation of the raw data and the experimental bias between 0 and 1.

tered by a 640 nm long pass filter. The detected light is then transferred by $2f-2f$ imaging, through a symmetric non-polarizing beam splitter towards two single photon detectors (Count, Laser Components). This configuration reduces the avalanche photodiode (APD) cross talk significantly.

The sample is a mm-sized diamond which hosts nitrogen-vacancy-centers at natural abundance. For high excitation and collection efficiency of the NV-center a solid-immersion lens was fabricated around an earlier confocally localized center. Further details on its manufacture are presented elsewhere[24]. The centers and the solid-immersion lenses are identified by confocal beam scanning. This was performed initially to locate the centers, but also in the course of the experiment the beam is repeatedly ($\Delta t = 8$ min.) medially and laterally scanned across a certain area. Then, the NV-center is re-centered and the measurement is continued. This suppressed drift of the sample during the measurement time. One of the lateral images is presented in Fig. 1b.

All detection events are recorded on a commercial FPGA-based time-tagger (Swabian Instruments, Timetagger 20). The time-tagger is operated with a 100 ps time resolution and records all detector events. Since each produced click is recorded in a 128 Bit binary (64 bit which detector has clicked and 64 bit with the time in ps), we have recorded 832 GiB in the course of 7 days (to be specific: 608125 seconds). This data set is split to 179 files, which are analyzed below. This corresponds to an average count rate of approximately 91.7 kcps, which includes the refocusing periods, which display a reduced count-rate for the time of refocusing. Since the real-time count rate is about 100 kcps, then the time without refocusing is approximately 558000 s.

To prove that a single emitter has been observed and to show the single photon nature of the emitted photon stream, we analyze the anti-bunching of the photons in a Hanbury Brown and Twiss configuration (see also Fig. 1a). This is performed by correlating the recorded time-stamps of the two APDs in a start-multiple-stop fashion[28]. The corresponding anti-bunching curve is shown in Fig. 1e. It shows an anti-bunching "dip" below the value of $g^{(2)}(0) = 0.5$, which proves the single photon nature of the source. The timing resolution τ_{rs} for the start-stop event is 500 ps. Furthermore, the curve shows some bunching behavior due to the NV-centers' typical meta-stable state above the low excitation limit.

The entire experiment was prepared to operate without any human interaction. During the experiment the entire setup was covered with black out material. The above mentioned refocusing procedure helped to ensure reliable operation. A measurement of the peak count rates is presented in Fig. 1d. Still, some fluctuations are observed in the course of the recording. These are caused mostly by thermal drift of the table. Most notably the position of the pinhole, and both APDs are influenced. The relative position of the excitation focus also plays an important role. We like to note that the average count rate (above) was only measured as 91 kcps and not approximately 100 kcps as shown here. This results from the fact that the refocusing procedure reduces the count rate periodically.

The single photon nature is online monitored by the recording of the auto-correlation function. This is implemented such that each photon click of one channel is correlated with all clicks in a certain time span of the other detector. This is a start-multiple-stop correlation, which does not go down as other recordings which only consider start-stop events[28].

Experiment results. In the course of 7 days we have acquired 832 GiB data. This corresponds to 55796707904 bits raw data. And the detected photons in the reflected arm are associated with the outcome 1,

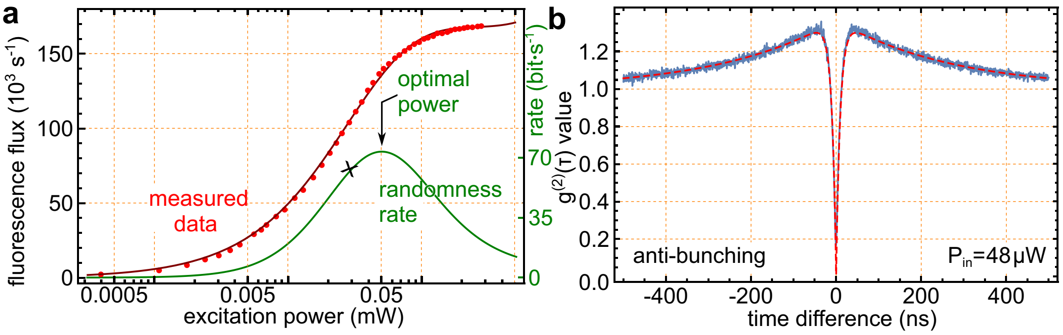

Figure 2. Entropy and Randomness Estimation. (**a**) Saturation curve of the utilized NV-center. To note the non-trivial behavior at higher laser powers, which indicate that the NV-center can not be considered as a simple three-level system. The optimal rate for the randomness generation speed is shown in green. This curve forms due to the fact that the anti-bunching curve gets narrower with an increasing laser power. This implies although more events are generated, the overall area below the curve is reduced. The cross in the green curve is the excitation power of the experimental data analyzed in supplementary material. (**b**) The anti-bunching curve at the optimal point of the randomness generator. The bottom at $\tau = 0$ amounts to $g^{(2)}(0) = 0.15$.

while the transmitted one are associated with the outcome 0. Then the number of zeros is 21753096536 bits, and the number of ones is 34043611368 bits. The integrated imbalance of the beam-splitter ratio and the detector efficiency amounts to probability $p(1) = 0.6101$, $p(0) = 0.3899$. This bias is indicated in Fig. 1e. Still, this bias is not necessarily a problem, since we assume the bits as still to be independent from each other. This is justified since the average waiting time between two photon detection events is considerably far away from the dead-time of the utilized single photon detectors. Furthermore, the given imbalance does only lead to a few percent reduction of the final entropy rate.

Still, this bias will largely decrease the usability of the random bits. We need to post-process the raw randomness bits and make them well balanced. When unbiasing the raw bits by two universal hashing, the conditional min-entropy is calculated by Eq. (4). $H_\infty(X|Y)$ gives us a conservative bound, which is how many random bits can be extracted per raw bit.

In our case, when considering the 11.5σ error bound, $H_\infty(X|Y)$ is 0.5559 bits, which means for per raw bit, 0.5559 bits secured random number can be extracted. With this value, by two universal hashing, we can get approximate 3.10×10^{10} unbiased random bits from the raw bits. The output speed of these unbiased random bits is 5.10×10^4 bits per second, when the refocusing periods where the count-rate is lowered are still counting as randomness generation time.

By limiting the generated raw random data to single photon events in the second model, we can guarantee the independence from uncorrelated background in the random data. Using Eq. (5), with 11.5σ error bound, the extractable quantum randomness from each raw bit amounts to 0.5168 bits. For the whole raw bits, the extractable quantum random bits are 2.88×10^{10} bits. When including the refocusing periods, the output speed of the quantum random number generator amounts to 4.74×10^4 bits per second.

Note that this quantum random number generation speed is smaller than the unbiased random bits generation speed in the first model. The difference between these two model indicates that in the first model, some background classical noise might have been considered as random events.

Next, we calculate the extractable quantum random bits from the perspective of the third model, which gives us some extended independence of an eavesdropper.

The fluorescence counts and the shape of anti-bunching curves are affected by the excitation power. Subsequently, R_{rand} depends on the excitation power to the single quantum emitter. As shown in Fig. 2a, the green curve is the quantum randomness output rate; it depends on different excitation powers. The curve has an optimal excitation power as expected. This stems from the fact that with an increase of the excitation power, the count rate of different detectors increases, while the shape of the anti-bunching curves becomes narrower, thus the green part in Fig. 3 would become smaller. At the given excitation intensity of 26 μW, the green part covers a range of $t = 10.55$ ns. When the excitation power is changed, the start-stop event count rate will first increase and later decrease. Subsequently, the quantum random bits output rate has an optimal operation point. For a simple three level system this rate matches with the saturation point of the utilized single photon emitter.

According to Eq. (6), we can calculate the quantum randomness output rate of our system before we post-process the raw random bits. The excitation power in the experiment is 26 μW. The integrated ratio of the beam splitter and the detection efficiency amounts as above to about 0.6101.

Following Eq. (7), with a very strict 11.5σ error bound, we compute the extractable quantum randomness per raw bit as 3.746×10^{-4}. With this value, after the randomness-extraction hashing, about 2.09×10^7 bits unbiased quantum random number can be extracted, and the quantum random number generation speed amounts to approximately 34.37 bits per second.

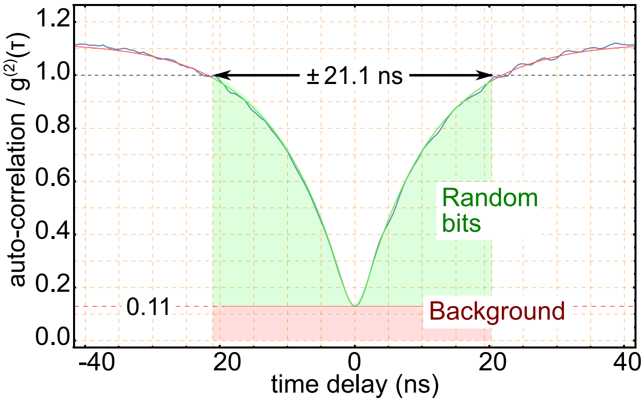

Figure 3. Anti-bunching as a Measure for Quantumness. The anti-correlation of photons is only observed in a small time interval. For the third randomness extraction model, the area of the generated bits between the classical bound of $g^{(2)}(\tau) \leq 1.0$ and above the background level are considered. This reduces the amount of raw input bits from the generator dramatically.

Conclusion and Outlook

In conclusion, we have theoretically described and experimentally implemented a random bit generator based on single photons which are impinging on a beam-splitter. The utilized single photon source is based on a single defect center in diamond. The generator is operated continuously over the course of one week and all detector events are recorded as time-tags, such that they could be conveniently post-processed.

The detection of raw random bits, which are associated with the output ports of the beam-splitter to ones and zeros result in a raw-bit stream. This has a number of subtleties. The single photon detection process is prone to technical effects such as the beam-splitter ratio, electrical dead-times and jitter. As with any other randomness generator, the raw bits can subsequently not been used without post-processing. Therefore an entropy analysis for the raw random bit stream was presented. In a further analysis, this model can be extended to estimate the amount of unwanted, and potentially untrusted background events. This estimation is based on the parameters of the recorded photon correlation function.

In a third method, only tuple detection events on changing bits are considered as raw bits. The limitation is further reduced to auto-correlation values below unity, and excluded the uncorrelated background. This selection, a subset of detection events, certifies the quantum nature of the source. Despite this quantum nature, the "decision" the experimental outcome is based on the fair-sampling assumption of the beam-splitter. Therefore, the fundamental randomness process is not tied to the quantum nature of the source. In this sense also any other input light source might sample the vacuum fluctuations at the empty beam-splitter port, which will be the relevant entropy source of such beam-splitter based generators, while the quantum input state only certifies the "quantumness" of the utilized light source.

By an estimation of the underlying entropy of this conservative model, which is bound to the knowledge of an external adversary, we can estimate the quantum randomness per raw bit is 3.746×10^{-4} bits. This fraction is used as input parameter for a randomness extraction. Then, the random bits are extracted. The final quantum random number generation speed is then about 34.37 bits per second.

Received: 23 May 2019; Accepted: 6 November 2019;
Published online: 05 December 2019

References

1. Lenstra, A. K. *et al.* Ron was wrong, Whit is right. *IACR*, http://eprint.iacr.org/ (2012).
2. Becker, G. T., Regazzoni, F., Paar, C. & Burleson, W. P. Stealthy dopant-level hardware trojans. In *International Workshop on Cryptographic Hardware and Embedded Systems*, 197–214 (Springer, 2013).
3. Young, A. & Yung, M. The dark side of "black-box" cryptography or: Should we trust capstone? In Koblitz, N. (ed.) *Advances in Cryptology — CRYPTO'* 96, 89–103 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1996).
4. Schmidt, H. Quantum-mechanical random-number generator. *Journal of Applied Physics* **41**, 462–468, http://link.aip.org/link/?JAP/41/462/1 (1970).
5. Erber, T. & Putterman, S. Randomness in quantum mechanics – nature's ultimate cryptogram? *Nature* **318**, 41–43 (1985).
6. Rarity, J. G., Owens, P. C. M. & Tapster, P. R. Quantum random-number generation and key sharing. *Journal of Modern Optics* **41**, 2435–2444, https://doi.org/10.1080/09500349414552281 (1994).
7. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. & Zbinden, H. Optical quantum random number generator. *Journal of Modern Optics* **47**, 595–598, https://doi.org/10.1080/09500340008233380 (2000).
8. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Review of Scientific Instruments* **71**, 1675–1680, http://link.aip.org/link/?RSI/71/1675/1 (2000).
9. Trifonov & Vig. Quantum noise random number generator (2007).
10. Shi, Y., Chng, B. & Kurtsiefer, C. Random numbers from vacuum fluctuations. *Applied Physics Letters* **109**, 041101, https://doi.org/10.1063/1.4959887 (2016).
11. Steinle, T., Greiner, J. N., Wrachtrup, J., Giessen, H. & Gerhardt, I. Unbiased all-optical random-number generator. *Phys. Rev. X* **7**, 041050, https://doi.org/10.1103/PhysRevX.7.041050 (2017).
12. Xu, F. *et al.* Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express* **20**, 12366–12377, http://www.opticsexpress.org/abstract.cfm?URI=oe-20-11-12366 (2012).

13. Abellán, C. *et al.* Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express* **22**, 1645–1654, http://www.opticsexpress.org/abstract.cfm?URI=oe-22-2-1645 (2014).
14. Colbeck, R. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. Ph.D. thesis, University of Cambridge (2009).
15. Pironio, S. *et al.* Random numbers certified by bell's theorem. *Nature* **464**, 1021–1024, https://doi.org/10.1038/nature09008 (2010).
16. Lunghi, T. *et al.* Self-testing quantum random number generator. *Phys. Rev. Lett.* **114**, 150501, https://doi.org/10.1103/PhysRevLett.114.150501 (2015).
17. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004, https://doi.org/10.1103/RevModPhys.89.015004 (2017).
18. Bronner, P., Strunz, A., Silberhorn, C. & Meyn, J.-P. Demonstrating quantum random with single photons. *European Journal of Physics* **30**, 1189, http://stacks.iop.org/0143-0807/30/i=5/a=026 (2009).
19. Branning, D. & Bermudez, M. Testing quantum randomness in single-photon polarization measurements with the NIST test suite. *J. Opt. Soc. Am. B* **27**, 1594–1602, http://josab.osa.org/abstract.cfm?URI=josab-27-8-1594 (2010).
20. Gräfe, M. *et al.* On-chip generation of high-order single-photon w-states. *Nature Photonics* **8**, 791–795, https://doi.org/10.1038/nphoton.2014.204 (2014).
21. Gruber, A. *et al.* Scanning confocal optical microscopy and magnetic resonance on single defect centers. *Science* **276**, 2012–2014, http://science.sciencemag.org/content/276/5321/2012 (1997).
22. Kurtsiefer, C., Mayer, S., Zarda, P. & Weinfurter, H. Stable solid-state source of single photons. *Phys. Rev. Lett.* **85**, 290–293, https://doi.org/10.1103/PhysRevLett.85.290 (2000).
23. Brouri, R., Beveratos, A., Poizat, J.-P. & Grangier, P. Photon antibunching in the fluorescence of individual color centers in diamond. *Opt. Lett.* **25**, 1294–1296, http://ol.osa.org/abstract.cfm?URI=ol-25-17-1294 (2000).
24. Jamali, M. *et al.* Microscopic diamond solid-immersion-lenses fabricated around single defect centers by focused ion beam milling. *Review of Scientific Instruments* **85**, 123703, https://doi.org/10.1063/1.4902818 (2014).
25. Beveratos, A. *et al.* Single photon quantum cryptography. *Phys. Rev. Lett.* **89**, 187901, https://doi.org/10.1103/PhysRevLett.89.187901 (2002).
26. Jacques, V. *et al.* Experimental realization of wheeler's delayed-choice gedanken experiment. *Science* **315**, 966–968, http://science.sciencemag.org/content/315/5814/966 (2007).
27. Abe, N., Mitsumori, Y., Sadgrove, M. & Edamatsu, K. Dynamically unpolarized single-photon source in diamond with intrinsic randomness. *Scientific Reports* **7**, 46722–, https://doi.org/10.1038/srep46722 (2017).
28. Oberreiter, L. & Gerhardt, I. Light on a beam splitter: More randomness with single photons. *Laser & Photonics Reviews* **10**, 108–115, https://doi.org/10.1002/lpor.201500165 (2016).
29. Paul, H. Photon antibunching. *Rev. Mod. Phys.* **54**, 1061–1102, https://doi.org/10.1103/RevModPhys.54.1061 (1982).
30. Loudon, R. *The quantum theory of light* (OUP Oxford, 2000).
31. Renner, R. & Wolf, S. Simple and tight bounds for information reconciliation and privacy amplification. In Roy, B. (ed.) *Advances in Cryptology - ASIACRYPT 2005*, 199–216 (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005).
32. Renner, R. & Koenig, R. Universally composable privacy amplification against quantum adversaries. *eprint arXiv:quantph/0403133*, quant-ph/0403133 (2004).
33. Fox, M. *Quantum Optics: An Introduction* (Oxford University Press, 2006).

Acknowledgements

We acknowledge useful comments from Prof. R. Renner, ETH Zurich. We further acknowledge the funding from the MPG, the SFB project CO.CO.MAT/TR21, ERC (Complexplas), the BMBF, the Eisele Foundation, the project Q.COM, and SMel. Also the network IQ^{ST} is acknowledged for funding.

Author contributions

I.G. and J.N.G. conceived the experiment(s), I.G. and X.C. conducted the experiments, X.C. analysed the results. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41598-019-54594-0.

Correspondence and requests for materials should be addressed to I.G.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.