EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH   **Open Access**

Independent quality assessment of a commercial quantum random number generator

Mikhail Petrov[1,2]* iD, Igor Radchenko[3], Damian Steiger[4,5], Renato Renner[4], Matthias Troyer[4,5] and Vadim Makarov[1,6,2,7]

*Correspondence: m.petrov@rqc.ru
[1]Russian Quantum Center, Skolkovo, Moscow, 121205, Russia
[2]NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, 119049, Russia
Full list of author information is available at the end of the article

Abstract

We reverse-engineer, test and analyse hardware and firmware of the commercial quantum-optical random number generator Quantis from ID Quantique. We show that > 99% of its output data originates in physically random processes: random timing of photon absorption in a semiconductor material, and random growth of avalanche owing to impact ionisation. Under a strong assumption that these processes correspond to a measurement of an initially pure state of the components, our analysis implies the unpredictability of the generated randomness. We have also found minor non-random contributions from imperfections in detector electronics and an internal processing algorithm, specific to this particular device. Our work shows that the design quality of a commercial quantum-optical randomness source can be verified without cooperation of the manufacturer and without access to the engineering documentation.

1 Introduction

Random number generators (RNGs) are used in a large variety of applications. Nowadays both software and physical RNGs are in use [1]. A crucial aspect of random numbers is their unpredictability—the outcome of a coin toss would not be considered random if it could be known before the tossing. Software RNGs do not satisfy this criterion (unless further assumptions are made) for their output is generated by a deterministic algorithm, which is why they are also termed "pseudo-random" [2]. Conversely, the output of physical RNGs is obtained by measuring physical quantities. According to quantum theory, for a suitably designed measurement on a quantum system, the outcome cannot be predicted even if the system's physical state at the time when the measurement process is started is known completely. Quantum RNGs exploit such quantum measurements. Hence, if designed properly, their outputs are fundamentally unpredictable and, in this sense, truly random [3].

Although physical RNGs are used in commercial applications, as of yet there does not exist any complete and reliable procedure for their certification [1]. Attempts to establish requirements based exclusively on an analysis of the output stream like NIST's tests [4] are

Springer

not sufficient to ascertain randomness, because a statistical test of a sequence can never prove its unpredictability [5]. Indeed, a device may pretend to generate randomness while actually replaying a bit sequence that has been prerecorded from a true random source. The output of such a fake RNG would then obviously pass any statistical test that the true random source passes, whereas a third party may hold an exact copy of the prerecorded sequence and hence predict its output.

There are in principle two different approaches to resolve this problem. One is device-independent random number generation [6–8]. Here the idea is to consider data generated by two separated devices that share quantum entanglement. The quantum origin of the data can then be certified by a Bell test. The advantage of this approach is that no assumptions about the inner workings of the devices that produce the data are necessary. However, with today's technology, device-independent schemes are complex lab experiments with impractically low bit rates (see, e.g., [9]). In addition, they still need some trusted randomness as input, which is used for selecting between the different observables that enter the Bell test.

Semi-device-independent QRNG [10] is a more technically feasible approach than device-independent. In return for the relative simplicity of the QRNG implementation and increase generation rate, the semi-device-independent QRNG requires some assumptions about the device operation or its features, although still does not need a complete device model. As example, some semi-device-independent protocols require that QRNG should have trusted source [11, 12] or trusted measurement [13, 14]. Other protocols do not require any assumptions for setup components, but they make assumptions on the overlap [15] or the energy [16] of the prepared quantum states or assumptions on the Hilbert space dimension [17, 18]. While generation rate increased significantly, technical realization of the semi-device-independent QRNG remains relatively complex and there are still no on-shelf devices.

In this work we are concerned with the converse, i.e., the device-dependent, approach [19]. In contrast to the above, device-dependent RNGs are more practical, smaller, faster, and cheaper [3]. The price to pay for this is that, to certify their unpredictability, one requires an accurate and verifiable model of the device's operation, described within the formalism of quantum theory. Such a description is however rarely available for real-world devices. In this case the assessment of the quality of the generated randomness may still be based on tests of the individual components of the device, but must usually be supplemented by strong assumptions about the parts that cannot be analysed completely.

Here we carry out such an analysis for the quantum-optical "Quantis" device from ID Quantique [20], which has been available since the year 2001 and used in a number of real-world applications (Swiss Lottery, United Kingdom NSI Banking, Ukraine Online Gaming, etc. [20]). As explained above, the question whether the device generates true randomness cannot be answered by mere statistical tests of the output sequence. Instead, a user must trust that the randomness-generating process the device's manufacturer claims to employ has been implemented correctly. To establish this trust, it should be possible for an independent party to examine and verify the generator, including an in-depth inspection of its internal functioning. This certification can be commissioned by the manufacturer from an accredited certification lab. ID Quantique has got verified the compliance of Quantis with the AIS 20/31 standard [21, 22].

Typically, in the course of such a certification, the lab examines design documentation provided by the manufacturer, and examines a device sample according to procedures defined in the standard. However, it is not clear how well the procedures in the existing standards cover the greater number of physical phenomena in the quantum RNG. Therefore, here we perform an independent examination of Quantis without access to the manufacturer's internal documentation. The goal of our work is to identify the physical processes that produce data in Quantis, and verify that the internal post-processing of this data is sound. Our analysis and model are specific to this particular type of device. Other types of QRNGs would have a different model and, possibly, other analysis approaches of their hardware, operation, and post-processing algorithms.

In analogue to existing practices in highly-demanding hardware-dependent areas [23, 24], the certification procedure of the physical RNG should consists of at least the following four stages.

- Discussion of the underlying physical model and assumptions.
- Examination of calculation algorithms.
- Inspection of the hardware realization.
- Statistical tests of the output bit stream.

We follow the above methodology in our study. Previous studies have only tested the output stream of Quantis [21, 25–27] but not analysed its internals.

We have examined 6 devices with different manufacturing dates, ranging from 2007 to 2013 with serial numbers (s/n): 0701100A210, 0701108A210, 0701132A210, 0902242A210, 1304527A210, and 1304609A210 (the first two digits represent the year of manufacture and the remaining digits are internal serial numbers). Our key sample that provides most of our data has been purchased from a regular stock, without warning the manufacturer of its intended use. We have been guided only by openly available information: a white paper [28], application note [29], user guide [20], randomness test report [27], and a patent that outlines the actual implementation of the optics [30]. These sources provide a very basic understanding of the device's principle and functionality. To obtain the rest of the necessary data, we have reverse-engineered the device, examining and analysing closely its electrical and optical parts. During the examination Quantis s/n 0902242A210 has been destroyed in order to explore its optical part, obtain images of avalanche photodiodes (APDs) and measure properties of the light source. Our key sample (s/n 1304527A210) has been disassembled but remained functional, and all our in-vivo measurements have been done on it. The other four samples (s/n 1304609A210, 0701100A210, 0701108A210, and 0701132A210) have not been disassembled and have only been used for tests of their output bit stream.

2 Quantis teardown

The basis of Quantis hardware is a printed circuit board (PCB) that carries all its construction elements. The board is coated with a thick layer of black epoxy then packed into a metal can, presumably either to hide the design or to protect internal components from ambient light and moisture. We have removed the can and epoxy by heating the PCB up to about 150 °C with a hot-air gun. At this temperature solder does not yet melt and electronic components survive, while the epoxy softens and can be peeled off completely. The PCB is shown in Fig. 1.
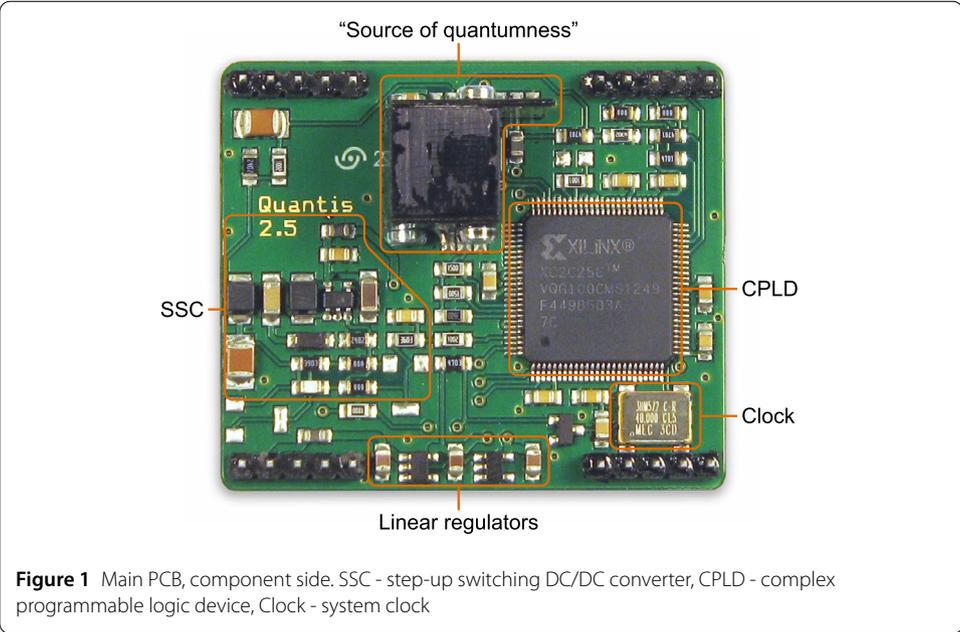
Figure 1 Main PCB, component side. SSC - step-up switching DC/DC converter, CPLD - complex programmable logic device, Clock - system clock
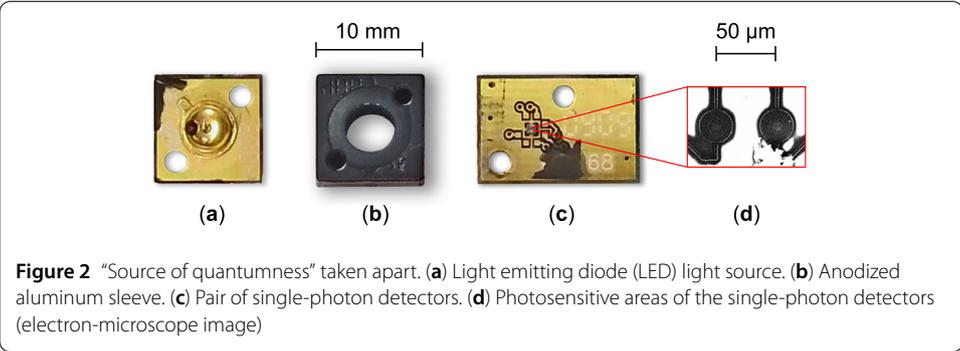
Figure 2 "Source of quantumness" taken apart. (**a**) Light emitting diode (LED) light source. (**b**) Anodized aluminum sleeve. (**c**) Pair of single-photon detectors. (**d**) Photosensitive areas of the single-photon detectors (electron-microscope image)

A key part of the device is its "source of quantumness", consisting of a black anodized aluminum sleeve [Fig. 2(b)] with a light source at one end [Fig. 2(a)] and a pair of single-photon detectors at the opposite end [Fig. 2(c)]. No optical beamsplitter element has been found inside the sleeve, which is consistent with the patent [30] but disagrees with the optical scheme included in the specification of the device that shows a free-space beam-splitter (Fig. 1 in [28]).

The detectors are avalanche photodiodes (APDs) working in a Geiger mode [31]. The all-silicon structure embodies a pair of APDs, amplifiers and quenching circuit for them. Geometric dimensions of the APDs have been determined by electron microscopy: the sensitive areas have a round shape with a diameter of $\approx 10\ \mu$m spaced at $50\ \mu$m between their centers [Fig. 2(d)]. A programmable step-up switching DC/DC converter (SSC) provides a bias voltage for both APDs.

We have measured spectral characteristics of the light source. It has broadband emission centered at 820 nm with full-width at half-magnitude (FWHM) of 40 nm, and viewing angle of 10°. These characteristics are very typical for a near-infrared light-emitting diode (LED).

Figure 3 Simplified electrical scheme of Quantis. A, amplifier; APD, avalanche photodiode; CNT, counter; CPLD, complex programmable logic device; GEN, clock generator; INT, integrator; LED, light emitting diode; NOR, inverted OR gate; PP, post-processing algorithm; R, resistor; SSC, switching power supply; XOR, exclusive OR gate

Figure 4 Signals in the circuit, recorded during normal operation. Trace names correspond to signal names in Fig. 3

Linear voltage regulators with 3.3 and 1.8 V output voltages (Fig. 1) power all on-board electronics. A broad-spectrum 40 MHz oscillator provides a system clock. A complex programmable logic device (CPLD) performs most of the device functionality. This CPLD is Xilinx type XC2C256 in a 100-pin package VQG100CMS1249 with multi-voltage input and output operation from 1.5 to 3.3 V. Unsurprisingly, the CPLD firmware is locked against its readout. All the following knowledge has therefore been obtained by analysing the rest of the electronic circuit, in-vivo signal capturing, applying external probing signals and observing them propagating through the circuit.

A simplified electrical scheme of Quantis and recorded real signals are shown in Figs. 3 and 4. The RNG works in a cycle-based regime. Every cycle starts with a 12 ns long voltage pulse formed at line *LD* by the CPLD [Fig. 5(a)], which is applied through a ballast resistor R to the LED causing it to emit a longer flash of light [Fig. 5(b)]. This light may trigger an avalanche in either of the APDs, generating, after amplification, "click" signals *DET1* and *DET2* for the CPLD. The CPLD operation procedure differs depending on whether or not clicks appear from the APDs. If none of the detectors has clicked, the CPLD just repeat next cycle by the pulse at line LD with a 50 ns delay (cycles # 2, 3, 7–9, 12, 14, ... in Fig. 4). If any of the APDs clicks, the CPLD *DETx* input goes high and it activates a quenching

Figure 5 Operation of the light source. (**a**) Voltage pulses applied to the LED from the CPLD, via line *LD*. (**b**) Light emitted by the LED

Figure 6 Post-processing state machine
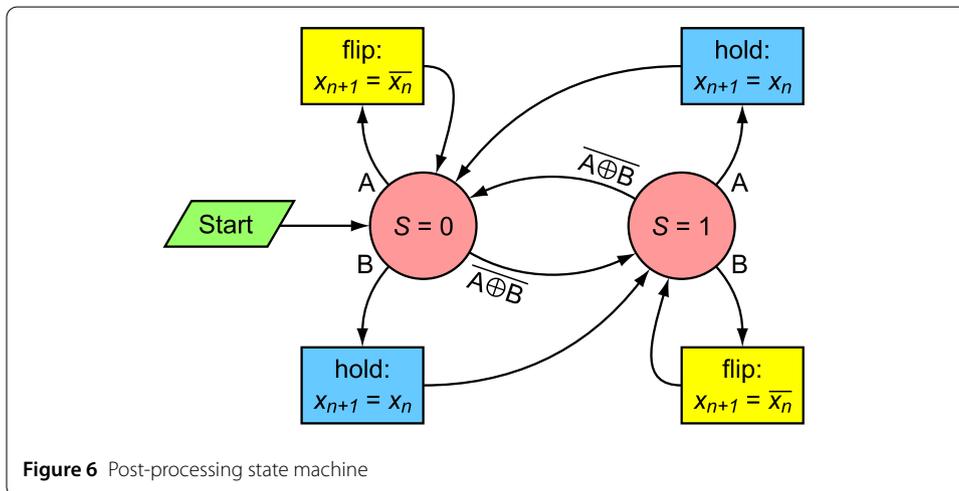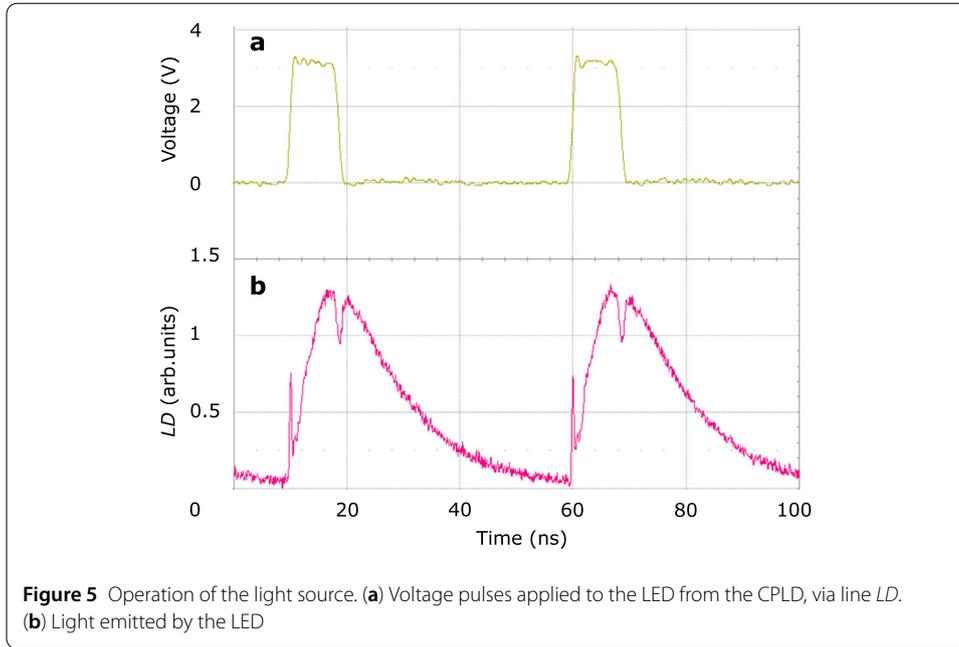
procedure by pulling the *QNCH* output low, which reduces the bias voltage V_b on both APDs and thus quenches the avalanche (cycles # 1, 4–6, 10, 11, 13, …). In most cycles with detectors clicks (cycles # 1, 4–6, 13, …) the CPLD starts next cycle with 150 ns delay presumably needed to reduce afterpulsing [31]. But sometimes one or both APDs click with a slight delay relative to the LED light pulse (cycles # 10, 11, 20), in these cases the post-processing algorithm (PP in Fig. 3) does not consider this to be a valid click and the cycle time remains 50 ns.

To convert input APD clicks into the output random bit stream, CPLD performs the post-processing procedure. After post-processing the output binary stream of the RNG is transmitted out through a serial peripheral interface (SPI) bus: the random bit value should be read on *data_out* line at the leading edge of the clock signal *data_sck* [29].

An analysis of the captured oscillograms reveals the following post-processing algorithm of converting APD clicks into the output stream. A random bit is output from PP if one

and only one APD clicks (cycles # 1, 4–6, 13, 15, 19, 23–25, 28 in Fig. 4), namely the output level *data_out* may change and a sync pulse *data_sck* is generated. In cycles when none (# 2, 3, 7–9, 12, 14, 16–18, 21, 22, 26, 29) or both (# 27) APDs click, and in cycles with delayed (# 10, 11, 20) APD clicks, no output random bit is produced (*data_out* remains unchanged and there is no sync pulse *data_sck*).

The post-processing consist of a state machine (Fig. 6). It has two states $S = 0$ and $S = 1$ and generates the output bit x_n (*data_out*) in each CPLD cycle n. Only one 1-bit internal variable exists: the value x_n of the last random bit outputted (0 or 1). Events A and B correspond to valid clicks of the first (*DET1*) and the second (*DET2*) APDs, respectively. The state machine works in every cycle as follows. When $S = 0$ and event A occurs, a "flip" is executed—the output bit value is reversed relative to the current one ($x_{n+1} = \overline{x_n}$) and the state S remains unchanged. When $S = 0$ and event B occurs, a "hold" is executed—the value of the output bit does not change ($x_{n+1} = x_n$) and the state S changes to the opposite (S becomes 1). When $S = 1$, at event A the hold occurs and at event B the flip occurs. In the cases when either none of the events A and B occur or both events A and B occur simultaneously, S changes to the opposite without outputting a bit. Note that PP treats delayed clicks (# 10, 11, 20) as the absence of A and B.

Figure 4 shows signals in the circuit well after the state machine has started. For the cycle we numbered #0 in Fig. 4 we have $S = 1$, $x_0 = 0$, and *data_out* = 0.

A feedback loop exists to maintain a mean rate of the output stream at the level of 4 MHz. For this purpose, the CPLD varies the bias voltage of the APDs V_b, effectively tuning their quantum efficiency (Fig. 3). A counter CNT measures a mean frequency of cycles when only one detector clicks. The error signal of the feedback loop is a difference between the value counted and the target rate of 4 MHz. The error signal passes through a software integrator INT and is applied to the voltage control input of the SSC.

3 Analysis of design

3.1 Physical model

We now have a closer look at Quantis' underlying physical model, which we describe in terms of standard notions from quantum optics. As we have investigated before, the light source is a LED with central line at $\lambda = 820$ nm and bandwidth of $2 \cdot \Delta\lambda = 40$ nm. For such a source the coherence time (a characteristic period of time while light wave "remembers" its history) can be estimated as

$$\tau_{\text{coh}} = \frac{\lambda^2}{2\pi c \cdot \Delta\lambda} \simeq 18 \text{ fs.} \tag{1}$$

On the other hand, the registration period of APDs signals is at least 25 ns $\gg \tau_{\text{coh}}$. Hence, the signal measured can be regarded a result of a large number of possible independent photon absorption events. This would imply that the APD clicks have Poissonian statistics and are independent in both channels.

No entanglement by the number of photons may exist in the current scheme: the presence or absence of a photon in one channel says nothing about signal in the other one. It contradicts the principle declared in ID Quantique Quantis white paper (p. 11) [28] that states it is a "which way" scheme. It is not, because registration of a photon in one channel does not exclude the possibility of photon registration in the other channel.

The actual physical source of randomness in Quantis is the photoexcitation of a carrier in the absorption layer of the APD [31]. A secondary significant source of randomness is the subsequent random growth of avalanche by impact ionisation in the APD [32]. Owing to the statistical nature of the latter process, some avalanches die without being detected (their number of carriers may fluctuate down to zero), and for those detected their detection time is randomly distributed.

Lacking a precise microscopic model of this hardware, we cannot however without further assumptions conclude that its apparent random behaviour is due to a generically unpredictable quantum process. At this point we thus need to make a crucial assumption. We suppose that the measured statistics of the data produced by the components would be unchanged if all degrees of freedom that are accessible to an adversary were initialised to any pure state. This assumption guarantees that a possible attacker who has access to information about the device's initial state cannot predict its outputs (beyond the bias implied by the measured statistics).

3.2 Post-processing procedure

Now, let us consider the post-processing algorithm with assumptions that follow from the physical model. We treat the signals from the pair of APDs as independent Poisson processes with different probabilities of clicks

$$\mathbb{P}(D_1) \equiv p_1, \qquad \mathbb{P}(D_2) \equiv p_2. \tag{2}$$

The probabilities of events when one and only one particular detector clicks (events A and B) are

$$
\begin{aligned}
\mathbb{P}(A) &= \mathbb{P}(D_1 \bullet \overline{D_2}) = p_1(1 - p_2) \equiv \alpha, \\
\mathbb{P}(B) &= \mathbb{P}(D_2 \bullet \overline{D_1}) = p_2(1 - p_1) \equiv \beta
\end{aligned}
\tag{3}
$$

and the probability that neither A nor B takes place is

$$\mathbb{P}(\overline{A + B}) = \mathbb{P}(\overline{D_1 \oplus D_2}) = 1 - \alpha - \beta. \tag{4}$$

In this notation the probability that the next output bit will be inverted with respect to the current bit (we call this action a flip) equals to

$$
\begin{aligned}
\mathbb{P}(\text{flip}) &= \alpha\big[\alpha + (1 - \alpha - \beta)\beta\big] \sum_{m=0}^{\infty}(1 - \alpha - \beta)^{2m} \\
&\quad + \beta\big[\beta + (1 - \alpha - \beta)\alpha\big] \sum_{m=0}^{\infty}(1 - \alpha - \beta)^{2m} \\
&= \frac{\alpha^2 + \beta^2 + 2\alpha\beta(1 - \alpha - \beta)}{1 - (1 - \alpha - \beta)^2},
\end{aligned}
\tag{5}
$$

where the sum over m is the probability of an even number of transitions between $S = 0$ and $S = 1$ without producing an output bit. Similarly, the probability of the next bit being

equal to the current bit (hold) is

$$\mathbb{P}(\text{hold}) = \alpha\big[\beta + (1 - \alpha - \beta)\alpha\big] \sum_{m=0}^{\infty}(1 - \alpha - \beta)^{2m}$$

$$+ \beta\big[\alpha + (1 - \alpha - \beta)\beta\big] \sum_{m=0}^{\infty}(1 - \alpha - \beta)^{2m} \qquad (6)$$

$$= \frac{2\alpha\beta + (\alpha^2 + \beta^2)(1 - \alpha - \beta)}{1 - (1 - \alpha - \beta)^2}.$$

Their difference is thus

$$\mathbb{P}(\text{flip}) - \mathbb{P}(\text{hold}) = \frac{(\alpha - \beta)^2}{2 - \alpha - \beta}$$

$$= \frac{(p_1 - p_2)^2}{2 - p_1 - p_2 + 2p_1 p_2} \geq \frac{(p_1 - p_2)^2}{2}. \qquad (7)$$

For a real physical system, the count probability of two detectors can never be perfectly equal, owing to differences in their quantum efficiency, size, intensity of illumination, and possibly other factors. It follows from Eq. (7) that if the probabilities of APD signals p_1 and p_2 are not exactly equal, then the event flip will be more likely than hold. This intrinsic property of the PP introduces correlations in the output stream, i.e., makes it less than perfectly random. We have studied this effect experimentally in Sect. 4.4.

The prevalence of the flip events may also be caused by the APD signals being non-Poissonian, in particular their exhibiting afterpulsing. We have not considered this effect in our model.

3.3 Feedback loop stability

A feedback loop that maintains a constant bitrate of the output stream includes integrator INT and switching power supply SSC (Fig. 3), besides other elements. SSC has a passive filter network at its output with a time constant of 100 ms. This means that its frequency response decays by 20 dB per frequency decade at frequencies > 1.6 Hz. The integrator provides an additional slope of 20 dB per decade in the loop gain. Hence, the phase margin is not sufficient, which may lead to peaking and oscillation of the output stream bitrate.

Moreover, this feedback loop in theory allows that a lock situation may happen. With increasing reverse bias voltage V_b, the probability of APD clicks increases. However, only single-detection events are counted. The higher V_b is, the more simultaneous clicks in both detectors appear and these events will be discarded. The negative feedback may then turn into positive. This may in principle lead to the system locking at the maximum V_b.

4 Measurements

In order to test the ability of RNG Quantis to generate random sequences, we have carried out a number of measurements on both the source of randomness (the APDs) and post-processing procedure. The objective of each is to find and quantify possible non-random effects. Since we are measuring correlations at the APD outputs, we deem it unnecessary to check the stability and power of the LED emission. It is clear both APDs are working in the Geiger mode, although their photon detection efficiency may be rather low (we did

Figure 7 APD dark count rate for the two APDs
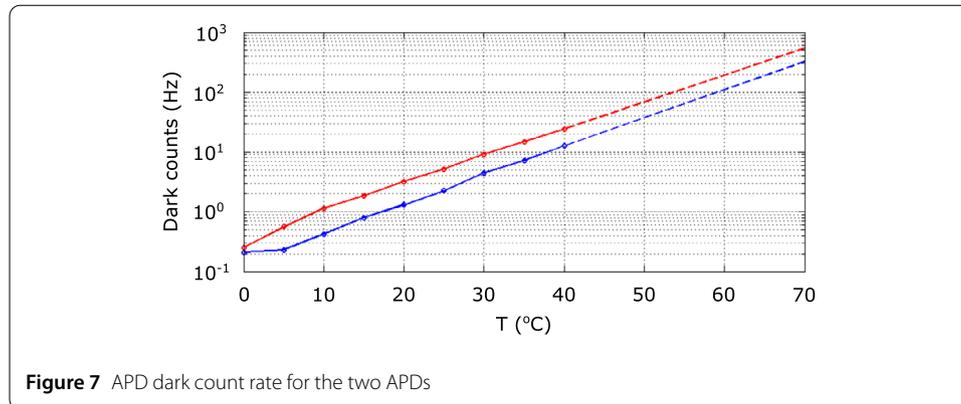
not measure it). We do not think low photon detection efficiency affects the randomness, because the physics of the avalanche remains the same. We compare the contribution of possible non-random effects in the output bit stream with the specification of Quantis that states that "thermal noise contribution" should be less than 1% [20], which means to be the upper bound on all potential non-randomness in the output stream. While we cannot claim that our set of measurements is complete, the sum of the non-random effects we have found does not exceed 1%.

4.1 Dark counts

Even in the absence of light, the APDs produce a certain number of clicks—dark counts [31]. Conservatively, these are not considered to be the source of randomness.

We have measured the dark counts in 0 to 40 °C temperature range, by placing Quantis in a thermal chamber. Results of the measurements are shown in Fig. 7. The dark count rate rises exponentially with temperature. Extrapolating to +70 °C, which it a commonly assumed upper end of operating temperature range for commercial products, we obtain less than 1 kHz dark count rate summed over the two APDs. Thus the dark counts contribute less than 0.025% of the output bits.

4.2 Autocorrelation of APD counts

In Quantis the sources forming a random output sequence are APDs. Therefore, we have first studied the properties of the output signals obtained from photodetectors directly after their pre-amplification (*DET1* and *DET2* in Fig. 3).

As discussed in Sect. 3.1, the clicks from each photodetector should be independent and their statistics should be Poissonian. The measured autocorrelation function under continuous-wave illumination from the LED is plotted in Fig. 8(a). It has an expected shape for a Poissonian process, with a dip in the first 150 ns owing to the deadtime imposed by the PP. However a close examination reveals small-amplitude oscillation of unknown origin, which we have magnified in Fig. 8(b). The peak-to-peak magnitude of these oscillations reaches 2.6%.

Owing to the relatively large magnitude exceeding 1% and the oscillation frequency comparable with the output bit rate, this effect is potentially significant. To analyse it, the measurement needs to be repeated in the normal operation of the circuit (with gated LED). Also, a cross-correlation on a similar or longer time scale need to be measured and the combined correlation propagated through the PP. Unfortunately, we have realised this

Figure 8 Autocorrelation of APD clicks under continuous-wave illumination, for the two APDs (red and blue). (**a**) Plot on the log scale. (**b**) Deviations of the measured data from an exponential fit (or linear fit of the log plot). The measurement time was 1000 s
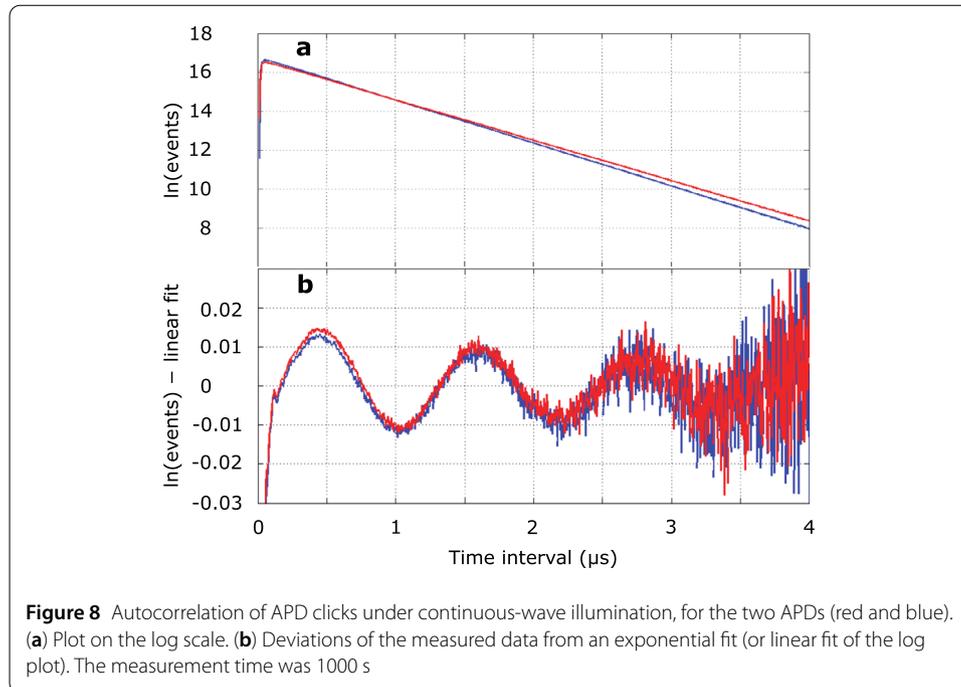
after dismantling the experiment. A simpler cross-correlation measurement presented in Sect. 4.3 is insufficient for this analysis.

4.3 Cross-correlation of APD counts

During an avalanche, the APD emits a few photons, so-called backflash [33]. These may reach the other APD (via internal reflections and scattering inside the optical enclosure shown in Fig. 2) and cause a correlated click. Also, electronic interference between the two single-photon detector circuits may in principle exist. Such clicks are not considered to be random.

In order to estimate the click rate owing to the backflash, we have electrically disconnected the LED and measured cross-correlation between *DET1* and *DET2* in darkness (Fig. 9). The peak owing to the optical cross-talk is clearly visible. However, the probability of backflash-induced click is small: in 16 h measurement time, we have registered 2.8×10^6 single clicks in one APD and 4.3×10^6 in another, but only about 500 coincidences in ±20 ns window. Thus the contribution of the cross-talk to the output bit stream is $\approx 0.007\%$.

In order to check for possible further cross-talk effects, we have repeated the measurement under continuous-wave illumination from the LED. The result is shown in Fig. 10. The central features are caused by the expected circuit operation such as quenching (Sect. 2). However any cross-correlation beyond the shortest bit generation interval of ±150 ns would be of interest, because it may affect the output bit stream. Our histogram shows an elevated cross-correlation probability in -300 to -150 ns range, however a further study is required to confirm and quantify it.

4.4 Statistical imperfections in the output bit stream

To verify statistic bias owing to APD efficiency mismatch derived in Sect. 3.2, a dedicated FPGA-based circuit has been designed. It allows to analyse long consistent sequences in

Figure 9 APD cross-talk, measured in darkness over 16 h. Histogram bin size is 4 ns

Figure 10 Cross-correlations of APD clicks under continuous-wave illumination, measured over 3600 s. Histogram bin size is 4 ns
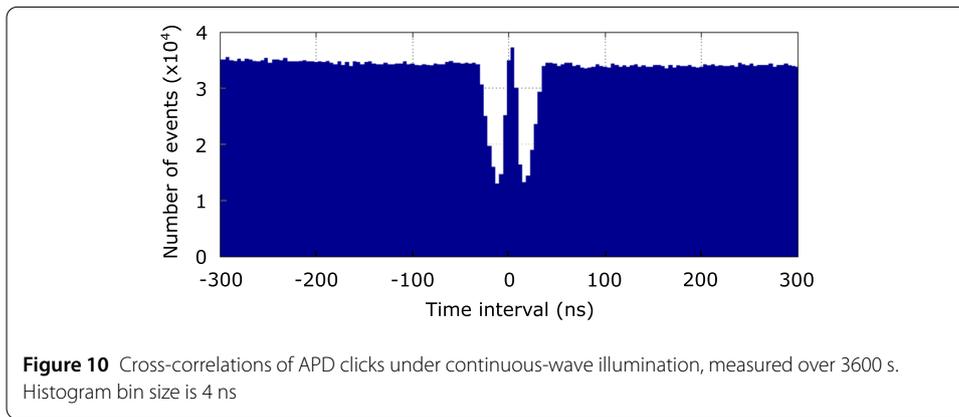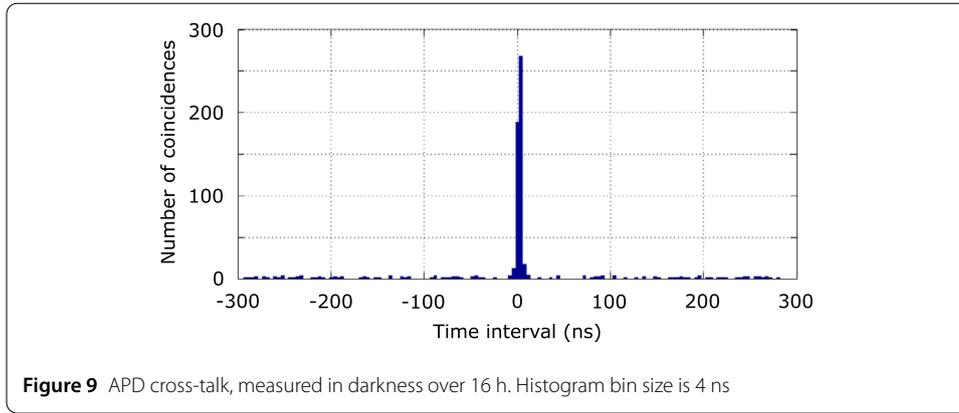
Table 1 Output stream statistics. Each sequence length $N = 1$ Gibit $(\equiv 2^{30}$ bit)

Quantis s/n	$\mathbb{N}(x_n = 0)$	$\mathbb{N}(x_n = 1)$	$\frac{\mathbb{N}(=1)-\mathbb{N}(=0)}{\mathbb{N}(=1)+\mathbb{N}(=0)}$	$\mathbb{N}(x_n \oplus x_{n+1} = 0)$	$\mathbb{N}(x_n \oplus x_{n+1} = 1)$	$\frac{\mathbb{N}(\oplus=1)-\mathbb{N}(\oplus=0)}{\mathbb{N}(\oplus=1)+\mathbb{N}(\oplus=0)}$
0701100A210	536,867,999	536,873,825	5.4×10^{-6}	536,828,388	536,913,435	7.9×10^{-5}
0701108A210	536,869,215	536,872,609	3.2×10^{-6}	536,839,365	536,902,458	5.9×10^{-5}
0701132A210	536,892,157	536,849,667	-4.0×10^{-5}	536,666,863	537,074,960	3.8×10^{-4}
1304527A210	536,882,563	536,859,261	-2.2×10^{-5}	536,787,990	536,953,833	1.5×10^{-4}
1304609A210	536,873,035	536,868,789	-4.0×10^{-6}	536,698,339	537,043,484	3.2×10^{-4}

real time without missing a bit. With this setup, the sequence of signals of $N = 1$ Gibit length at the output of the RNG has been analysed. The results of this analysis are given in Table 1. We have measured five devices with different s/n. For each device, we have counted the number of bits 0 and 1 in the output stream $\mathbb{N}$ and calculated their relative deviation from equiprobable. We have also counted the number of hold and flip events, i.e., the number of two consecutive bits having matching and not matching values. The last column shows the relative deviation of hold and flip from equiprobable.

For a large and perfectly random binary sequence, the standard deviation of the relative deviation from equiprobable is $N^{-1/2} \approx 3.05 \cdot 10^{-5}$. The relative deviation between the number of 0 and 1 bits in our tests is small and does not exceed the standard deviation, with the exception of the device s/n 0701132A210 that slightly exceeds it. These results are in good agreement with the expected equal probability of 0 and 1, i.e., the output sequence is balanced. However, for the hold and flip events the situation is different. Their measured

relative deviation exceeds the standard deviation by a factor of 2 to 12. We infer that this statistical deviation is due to APD efficiency mismatch.

Assuming click probabilities for both APDs are approximately equal $p_1 \approx p_2 \approx 0.28$ (estimated from the recorded oscillograms in Fig. 4), we obtain from Eq. (7):

$$\mathbb{P}(\text{flip}) - \mathbb{P}(\text{hold}) \approx \frac{(p_1 - p_2)^2}{2 - 2p_1 + 2(p_1)^2} \approx \frac{(p_1 - p_2)^2}{1.6},$$

$$|p_1 - p_2| \approx \sqrt{1.6\big[\mathbb{P}(\text{flip}) - \mathbb{P}(\text{hold})\big]}. \tag{8}$$

For Quantis s/n 0701132A210, in which the greatest deviation has been observed, the absolute difference of APD click probabilities $|p_1 - p_2| \approx 0.025$ and the relative difference $|p_1 - p_2|/p_1 \approx 8.8\%$. While this is a fairly good click rate matching for the APDs manufactured on the same chip, they are not identical.

We remark that the above statistically significant prevalence of the flip bit pairs over hold bit pairs has neither been detected by the manufacturer's statistical testing [27] nor our own application of the NIST SP800-22 test suite [34] on the output stream from our above-mentioned worst sample. It was detected by independent researchers [26], who however could not explain its origin. They tested a Quantis sample purchased in 2004 and also observed a statistically significant bias (fewer zeros than ones in the output sequence) that we did not observe in our samples.

4.5 Feedback signal
We have measured time and frequency characteristics of the feedback signal (Fig. 11). As expected, it exhibits oscillations with the spectral maximum around 33 Hz. These oscillations however should not affect the probability distribution of the output sequence, because they affect both APDs in the same way. However, they should cause the timing of the output bits to not be regular, which indicates that the timing should not be used in an application.

We have not observed the system locking, whose theoretical possibility is mentioned in Sect. 3.3.

5 Discussion and conclusion
While no optical beamsplitter element has been found in the Quantis device, it nevertheless contains two sources of randomness—two Geiger-mode APDs. Within them, the relevant quantum processes are photoexcitation and impact ionisation. Basically, either APD may be regarded as an independent source of randomness, however the presence of two of them increases the output bit rate. Indeed, a similar QRNG based on a single APD can be constructed [35].

To assess the quality of the randomness generated by these APDs, one would in principle need a microscopic model describing their workings. Within such a model, one may then attempt to prove that their output is unpredictable even if the quantum state of the APDs was fully known (i.e., pure) at the time when the randomness generation process is initiated, that is, when the device received the trigger signal requesting it to generate randomness [19]. However, lacking such a microscopic model, one may also resort to physically reasonable assumptions. Specifically, we assume here that the experimentally

Figure 11 Control input signal of SSC, in (**a**) time domain and (**b**) frequency domain
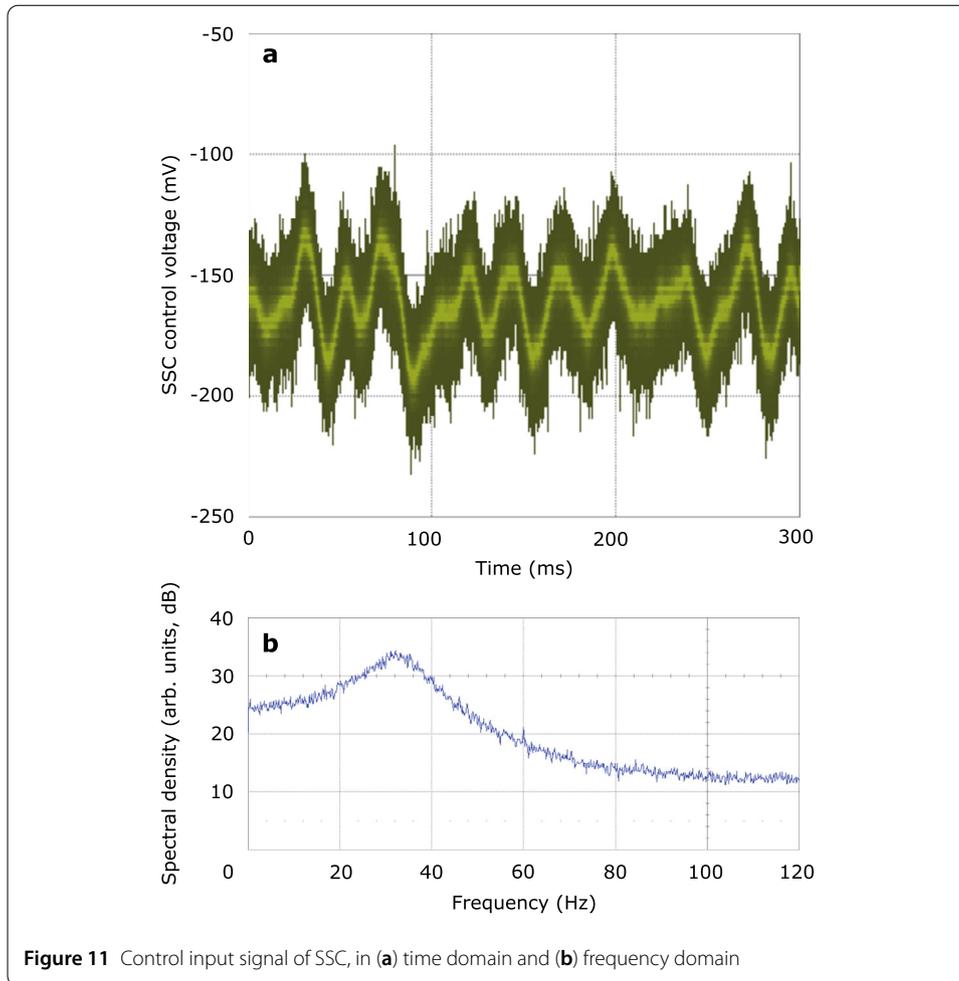
measured behaviour of the APDs is identical to the one they would exhibit if their microscopic degrees of freedom that are accessible to an adversary were at the beginning of each measurement in any pure state. Under the assumption that the adversary has no access to the device, this assumption holds trivially.

We have tested for potential imperfections in Quantis that could have an impact on the randomness in the output bit stream. We have found a correlation between adjacent output bits owing to the click rate mismatch of the APDs. However this and other effects stay well below the specified "thermal noise contribution" of less than 1% [20]. Our preliminary conclusion is that Quantis conforms to its published specification of the physical randomness content in the output bit stream, provided that one is ready to make the assumptions described above.

Unfortunately, one potential effect that may lead to an additional reduction of randomness—auto- and cross-correlations of APD clicks—has not been sufficiently well measured and analysed by us to reach a conclusion. This could be the topic of a future study.

We also note that the post-processing implemented by the device does not include randomness extraction. The generated randomness may thus be used for applications where a small bias is acceptable. However, for applications that require uniform randomness, the raw randomness generated by the device would need to be further processed by randomness extractors (see [36] for details). To choose the corresponding extractor parameters,

one would also need an estimate of the min-entropy of the raw randomness. Such an estimate would however require additional assumptions on the type of side information held by an adversary as well as a detailed analysis of cross-correlations, and thus goes beyond the scope of this work. We remark that not all applications require or indeed can tolerate the time-consuming randomness extraction. An example of the latter is testing for the violation of a Bell inequality with the locality and freedom-of-choice loopholes closed [37–39]. There, the short time between the photon absorption in the APD and the resulting random bit being used for measurement choice is a crucial experimental and conceptual constraint.

Overall, we have shown that an independent security analysis of a commercial quantum RNG can be done. This improves the trust in these devices.

We shared the finished manuscript with ID Quantique before its submission for publication. The company read it, thanked us, and did not suggest any significant corrections.

Declarations

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
MP finished the data analysis and finished writing the Article with input from all authors. IR performed all the experiments, hardware, and data analysis, and started writing the Article with input from all authors. DS and RR contributed to the data analysis. MT performed the initial hardware analysis and supervised the study. VM supervised the study. All authors read and approved the final manuscript.

Author details
[1]Russian Quantum Center, Skolkovo, Moscow, 121205, Russia. [2]NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, 119049, Russia. [3]Moscow State University, Moscow, 119991, Russia. [4]Institute for Theoretical Physics, ETH Zurich, CH-8093 Zurich, Switzerland. [5]Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA. [6]Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai, 201315, People's Republic of China. [7]Department of Physics and Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada.

Publisher's Note

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

References
1. L'Ecuyer P. History of uniform random number generation. In: Proc. winter simul. conference. IEEE; 2017. p. 202–30.
2. Knuth DE. The art of computer programming. 3rd ed. vol. 2. Boston: Addison-Wesley; 1997.
3. Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. Rev Mod Phys. 2017;89:015004.
4. Soto J. Statistical testing of random number generators. In: Proc. 22nd national inf. systems security conference. NIST; 1999. p. 321–32.
5. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S. A statistical test suite for random and pseudorandom number generators for cryptographic applications. 2010. NIST Special Publication 800-22 Revision 1a.
6. Colbeck R, Kent A. Private randomness expansion with untrusted devices. J Phys A. 2011;44:095305.
7. Pironio S, Acín A, Massar S, Boyer de la Giroday A, Matsukevich DN, Maunz P, Olmschenk S, Hayes D, Luo L, Manning TA, Monroe C. Random numbers certified by Bell's theorem. Nature. 2010;464:1021–4.

8.　Colbeck R, Renner R. Free randomness can be amplified. Nat Phys. 2012;8:450–3.

9.　Liu W-Z, Li M-H, Ragy S, Zhao S-R, Bai B, Liu Y, Brown PJ, Zhang J, Colbeck R, Fan J, Zhang Q, Pan J-W. Device-independent randomness expansion against quantum side information. Nat Phys. 2021;17:448.

10.　Pawłowski M, Brunner N. Semi-device-independent security of one-way quantum key distribution. Phys Rev A. 2011;84:010302.

11.　Nie Y-Q, Guan J-Y, Zhou H, Zhang Q, Ma X, Zhang J, Pan J-W. Experimental measurement-device-independent quantum random-number generation. Phys Rev A. 2016;94:060301.

12.　Cao Z, Zhou H, Ma X. Loss-tolerant measurement-device-independent quantum random number generation. New J Phys. 2015;17:125011.

13.　Vallone G, Marangon DG, Tomasin M, Villoresi P. Quantum randomness certified by the uncertainty principle. Phys Rev A. 2014;90:052327.

14.　Avesani M, Marangon DG, Vallone G, Villoresi P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. Nat Commun. 2018;9:5365.

15.　Brask JB, Martin A, Esposito W, Houlmann R, Bowles J, Zbinden H, Brunner N. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. Phys Rev Appl. 2017;7:054018.

16.　Rusca D, van Himbeeck T, Martin A, Brask JB, Shi W, Pironio S, Brunner N, Zbinden H. Self-testing quantum random-number generator based on an energy bound. Phys Rev A. 2019;100:062338.

17.　Lunghi T, Brask JB, Lim CCW, Lavigne Q, Bowles J, Martin A, Zbinden H, Brunner N. Self-testing quantum random number generator. Phys Rev Lett. 2015;114:150501.

18.　Mironowicz P, Cañas G, Cariñe J, Gómez ES, Barra JF, Cabello A, Xavier GB, Lima G, Pawłowski M. Quantum randomness protected against detection loophole attacks. Quantum Inf Process. 2021;20:39.

19.　Frauchiger D, Renner R, Troyer M. True randomness from realistic quantum devices. arXiv:1311.4547 [quant-ph].

20.　ID Quantique. Quantis random number generator, https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/, visited 3 Apr 2020.

21.　Walenta N, Soucarros M, Stucki D, Caselunghe D, Domergue M, Hagerman M, Hart R, Hayford D, Houlmann R, Legré M, McCandlish T, Page J-B, Tourville M, Wolterman R. Practical aspects of security certification for commercial quantum technologies. In: Proc. SPIE. vol. 9648. 2015. p. 96480U.

22.　ID Quantique. Quantis AIS 31 validated RNG. https://www.idquantique.com/random-number-generation/products/quantis-ais-31/, visited 3 Apr 2020.

23.　Youn W, Yi B. Software and hardware certification of safety-critical avionic systems: a comparison study. Comput Stand Interfaces. 2014;36:889–98.

24.　Kornecki AJ, Zalewski J. Hardware certification for real-time safety-critical systems: state of the art. Annu Rev Control. 2010;34:163–74.

25.　Calude CS, Dinneen MJ, Dumitrescu M, Svozil K. Experimental evidence of quantum randomness incomputability. Phys Rev A. 2010;82:022102.

26.　Abbott AA, Bienvenu L, Senno G. Non-uniformity in the Quantis random number generator. 2014. CDMTCS Research Reports CDMTCS-472.

27.　ID Quantique. Quantis randomness test report, Version 2.0. 2010. https://marketing.idquantique.com/acton/attachment/11868/f-004c/1/-/-/-/-/Randomness%20Test%20Report.pdf. visited 7 Dec 2019.

28.　ID Quantique. Random number generation white paper. 2019. https://marketing.idquantique.com/acton/attachment/11868/f-0226/1/-/-/-/-/What%20is%20the%20Q%20in%20QRNG_White%20Paper.pdf. visited 7 Dec 2019.

29.　ID Quantique. Quantis-OEM application note. https://marketing.idquantique.com/acton/attachment/11868/f-021e/1/-/-/-/-/Quantis%20OEM_Application%20Note.pdf. visited 7 Dec 2019.

30.　Ribordy G, Guinnard O. Method and apparatus for generating true random numbers by way of a quantum optics process. US patent US7519641B2 (granted in 2009, filed in 2004).

31.　Cova S, Ghioni M, Lotito A, Rech I, Zappa F. Evolution and prospects for single-photon avalanche diodes and quenching circuits. J Mod Opt. 2004;51:1267–88.

32.　Spinelli A, Lacaita AL. Physics and numerical simulation of single photon avalanche diodes. IEEE Trans Electron Devices. 1997;44:1931–43.

33.　Renker D. Geiger-mode avalanche photodiodes, history, properties and problems. Nucl Instrum Methods Phys Res, Sect A. 2006;567:48–56.

34.　NIST SP 800-22: download documentation and software. https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software. visited 12 Apr 2021.

35.　Radchenko I. Preparation and measurement of quantum states in quantum communication protocols. Ph D thesis, AM Prokhorov General Physics Institute of the Russian Academy of Sciences. 2015. (in Russian).

36.　Troyer M, Renner R. ID Quantique technical paper on randomness extractor. version 1.0 (Sep 2012), available on request from https://www.idquantique.com/resource-library/random-number-generation/.

37.　Scheidl T, Ursin R, Kofler J, Ramelow S, Ma X-S, Herbst T, Ratschbacher L, Fedrizzi A, Langford NK, Jennewein T, Zeilinger A. Violation of local realism with freedom of choice. Proc Natl Acad Sci USA. 2010;107:19708–13.

38.　Hensen B, Bernien H, Dréau AE, Reiserer A, Kalb N, Blok MS, Ruitenberg J, Vermeulen RFL, Schouten RN, Abellán C, Amaya W, Pruneri V, Mitchell MW, Markham M, Twitchen DJ, Elkouss D, Wehner S, Taminiau TH, Hanson R. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. Nature. 2015;526:682–6.

39.　Hu X-M, Liu B-H, Guo Y, Xiang G-Y, Huang Y-F, Li C-F, Guo G-C, Kleinmann M, Vértesi T, Cabello A. Observation of stronger-than-binary correlations with entangled photonic qutrits. Phys Rev Lett. 2018;120:180402.