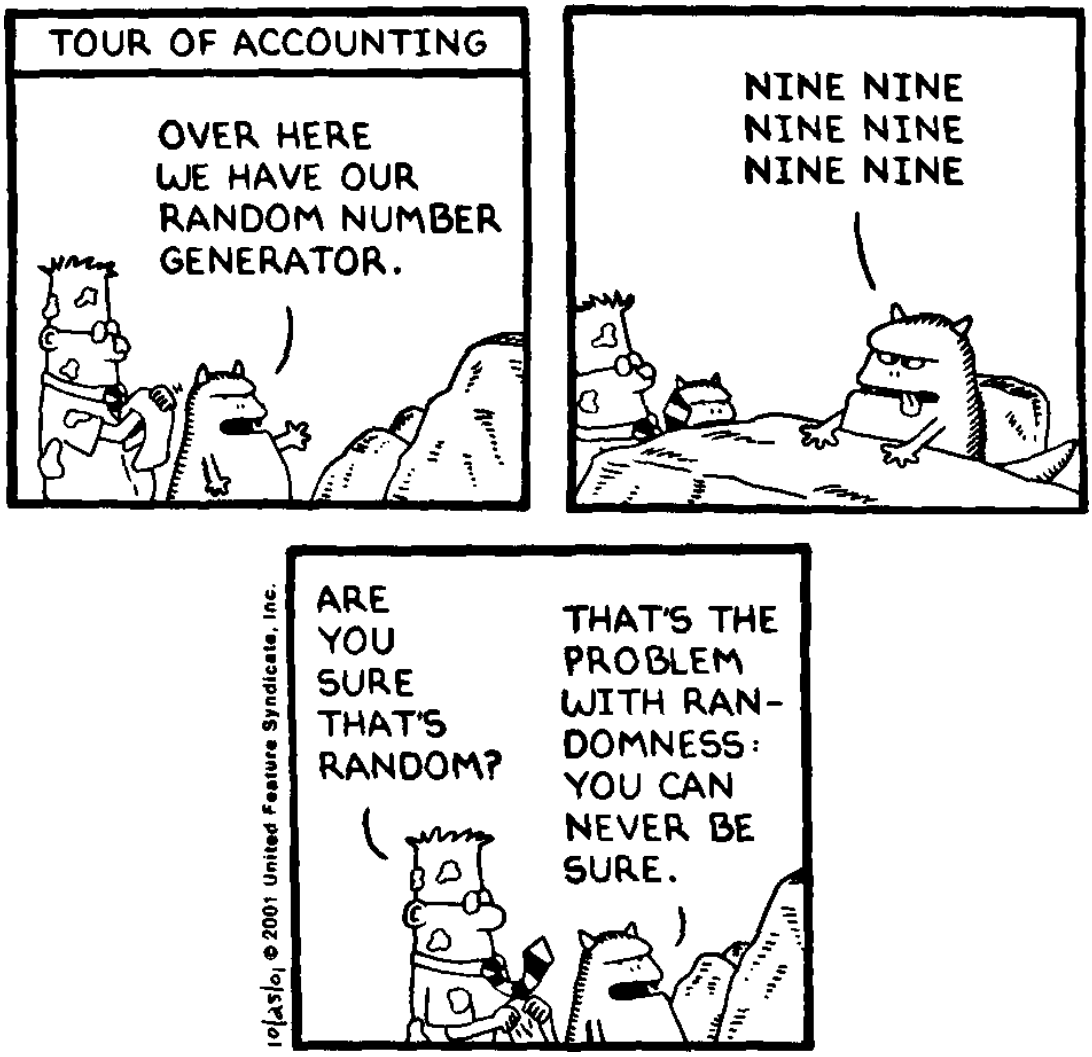
Lab manual:
Quantum random number generator

Dmitry Shkrabin, Anastasiya Ponosova, Maxim Fadeev, Daniil Trefilov,
Alexey Abrikosov, Elena Anisimova, Vadim Makarov, and Roman Shakhovoy
(Dated: April 5, 2025)



I. OBJECTIVES

This lab work teaches the students the design of optical quantum random number generators (QRNGs) and analysis of their characteristics, including the randomness of a bit sequence. Our lab QRNG is based on the interference of laser pulses. During the exercise, the students learn to operate laboratory instruments (oscilloscope, pulse generator, etc.).

II. PREREQUISITES AND OUTLINE

This lab exercise requires a basic understanding of random number generators (RNGs) classification and principles of their operation, including the term "entropy" in context of randomness estimating in the information theory. If you feel misunderstanding regarding these issues, here is an overview for background reading [1].

You will adjust the quantum random number generator based on pulse interference and extract and analyze a raw bit sequence. The implemented optical scheme simulates a commercially distributed QRate QRNG (Patent No US 11055404 B2 [2]). The must-read paper for successfully carrying out this lab exercise is [3]. It is appended to this manual. Please read it before you come to the lab.

In addition, you might take a look at papers [4, 5]. The paper [4] describes the basic operating principle of the optical scheme under study, and the papers [3, 5] present QRNG analysis and testing methodologies.

A. Outline

During this lab, you will learn how to analyze quantum RNG on the example of an optical scheme based on interference of laser pulses. The work progresses in the following four stages.

1. Setting up of hardware realization and measuring the output interference signal and its probability distribution.

2. Discussion of the underlying physical model and assumptions.

3. Data processing to extract bit sequences.

4. Statistical test of the output bit streams.

B. Questions for preparation

To check your understanding of the background, try answering the following questions. If you can not answer them, you need more preparation before you start the lab. Do not include your answers into the lab report.

– For a fiber-optic Mach-Zehnder interferometer with a path difference L, what pulse repetition rate f_p should be set for the first laser pulse to interfere with the second? With the third? With the n-th? How does the answer change for the Michelson interferometer?

– If the frequency in the unbalanced interferometer does not match the above condition, what is the intensity waveform at the output? Draw it.

– Should one consider polarization effects in Michelson interferometer?

– What is the source of randomness in QRNG based on the interference of laser pulses? How can you prove that the device generates true randomness?

– What physical quantity is measured to derive the true randomness in the lab work?

– What is the shape of the probability distribution of interference signal in the ideal case? What effects affect this distribution?

III. THEORY

A. Introduction into random number generators

Random numbers are a fundamental resource in science and engineering. They are essential for such important applications as cryptography, simulation, coordination in computer networks, etc. There are two main approaches to produce random numbers. The first one is based on computational deterministic algorithms. As any algorithmically generated sequence cannot be truly random, these methods are called pseudorandom number generators (PRNGs) [1]. PRNGs are popular in some applications owing to high-speed, low cost, and reproducibility; however, they usually cannot provide unpredictability, which is requisite for sensitive fields like information security.

Another approach to RNG is utilizing some unpredictable or, at least, difficult to predict physical process, measuring it to create a sequence of random numbers. These are called true random number generators (TRNGs). Quantum number generators are a particular case of physical TRGNs, whose output is the result of quantum events. QRNGs leverage the probabilistic nature of quantum mechanics to generate unbiased sequences of random numbers from fundamentally non-deterministic processes. Various physical phenomena have been employed in QRNG implementations, including measurements of radioactive decay, absorption of single photons, vacuum noise, energy fluctuations of stimulated Raman scattering, and superposition states of single photons.

The particular physical quantity we will use in this class is the phase of electric field in the laser pulses. This quantity is determined by quantum fluctuations of the vacuum, which are truly random and have a very short correlation time.

The theory part of the lab manual is organized as follows. First, a brief explanation of randomness is given, and requirements on random numbers are derived. Next, we discuss the QRNG certification procedure. Then, the structure of our QRNG device is explained. Finally, we overview test tools to probe the quality of random bit sequences.

B. Requirements on random numbers

Let us first understand what it means when a number is random. While it may not be immediately apparent, randomness is a highly non-trivial concept. Here is a simple explanation.

The attribute of being random applies more correctly to a sequence of numbers—without loss of generality, assuming just the bit values 0 and 1—rather than to individual numbers. Randomness is strictly related to the lack and, ideally, ***impossibility of predictability***. A simple test can be used to see if a sequence of numbers is random or not: compress it using zip compression on a PC. If you can compress a file of data, and it shrinks in size, it means that the compression tool found a recurring pattern in the data, removed redundant information, and plans to add it back later during decompression. There is predictability in the data, which therefore is not random.

In this sense, it might be better to speak of the randomness of a source. Ideally, one would like to have access to a source that produces random-bit strings, where the values of the bits can be described by ***independent and identically distributed (i.i.d.)*** random variables: the value of each bit is independent of past or future bit values, and it is 0 or 1 with the same probabilities as the other bits. The best scenario would be one where each bit is unbiased–that is, equally likely to be 0 or 1.

It is nearly impossible to establish whether a source of bit strings is actually random. As long as an i.i.d. source is not constant, that is, as long as it does not produce exclusively 0s or 1s, any output bit string of whatever fixed length can be generated, including those that contain only 1s or only 0s. Indeed, in the case where the i.i.d. source is unbiased, any string of the same length is equally probable. For example, the strings 00000, 11111, and 01001 are all equally probable.

Here, then, is the challenge: suppose our source produces a specific string. How can we be at least confident that the source is actually random, if any string is equally likely? The answer is that there are other properties of the string that we can analyze. For example, we can try to identify patterns or global properties, like the weight of the string, that is, how many 1s it contains. While all strings may be equally likely, their weight is not. If the source is really i.i.d., then we expect that, for long enough strings, with overwhelming probability, we will observe a string that is typical, that is, in the case of an unbiased source, that the number of 0s and 1s in it will be about the same. As an example of a pattern, imagine a source that alternates 0s and 1s. Considered individually, the bits may appear identically distributed and unbiased, but they are not independent: knowledge of the value of one bit and of the rule allows one to reconstruct all the other bits in the ordered string. This string is actually highly compressible.

The validation, or rather, corroboration of random sources, is typically performed with standardized tests that look for signs that the strings it produces exhibit some kind of pattern, ranging from an excess of 0s or 1s (that is, a bias) to correlations between various locations of the string.

One important measure of randomness is ***entropy***. Roughly speaking, it is the amount of information (measured in bits) necessary to describe a certain string among the set of all possible strings, or, equivalently, the amount

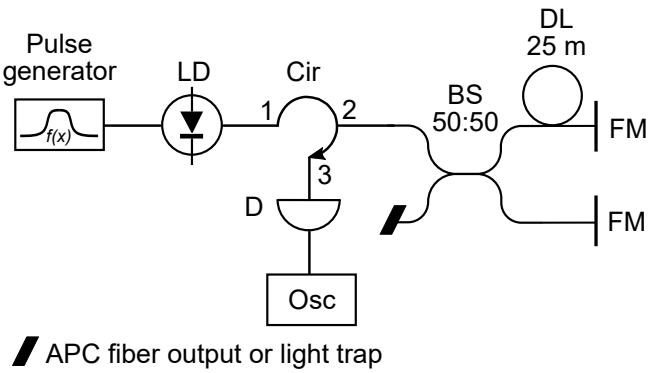


FIG. 1: Quantum RNG based on unbalanced Michelson interferometer. A pulse generator directly drives a distributed-feedback laser diode LD with electrical current. Cir, fiber-optic circulator; BS, fiber-optic beam-splitter; DL, delay line made of single-mode fiber; FM, Faraday mirror; D, fast p-i-n photodiode; Osc, oscilloscope.

of information gained when it is communicated which string was actually generated among the many possibilities. Roughly speaking, bit strings that are not random have limited entropy and can be described with fewer bits than the bit string contains. In the compression example above, this means that a file with high entropy will not compress and will remain the same size, whereas a file with low entropy will compress to a smaller file size.

Generally, the requirements on the random numbers depend on their intended application. Common criteria are that the random numbers should have good statistical properties, including uniformity and scalability. And for sensitive applications, their forward and backward unpredictability is indispensable. It means that the knowledge of subsequences of random numbers shall not enable to compute predecessors or successors or to guess them with non-negligible probability.

C. QRNG certification

A certification procedure should verify whether the QRNG satisfies the above-mentioned requirements. For statistical properties of generated bit sequences, many test suites are developed. However, they can never prove whether a sequence is unpredictable and answer whether the device generates true randomness. From the other side, using a quantum quantity as the entropy source does not guarantee good statistical properties of the bit sequence. Moreover, the QRNG device includes a post-processing stage, besides the entropy source. The measurement equipment and post-processing algorithms will also affect the statistical properties of the final bit sequence.

To validate all these requirements, the certification procedure of the physical RNG includes at least the following four stages [6].

– Discussion of the underlying physical model and assumptions.

– Examination of post-processing calculation algorithms.

– Inspection of hardware realization.

– Statistical test of the output bit steam.

D. Physical principle for entropy generation in QRNG based on interference of laser pulses

The schematic of our QRNG is shown in Fig. 1. Driven by a pulse generator, a distributed-feedback laser diode (LD) operates in gain-switching mode. It emits pulses at a wavelength $\lambda = 1550\ nm$ and a repetition frequency f_p. The pulses pass from the circulator (Cir) port 1 to port 2 into the Michelson interferometer. They divide at a coupler (BS), reflect from Faraday mirrors (FMs) and then recombine at BS again. Passing from circulator port 2 to port 3, the interference signal is detected in a time-resolved way by a photodiode (D). However, if a delay line of a length L is introduced into one of the interferometer arms, half of the original pulse arrives with a time delay $\Delta t = \frac{2L}{c}$ (hereon we refer to c as the speed of light in fiber, which is about 0.2 m/ns).

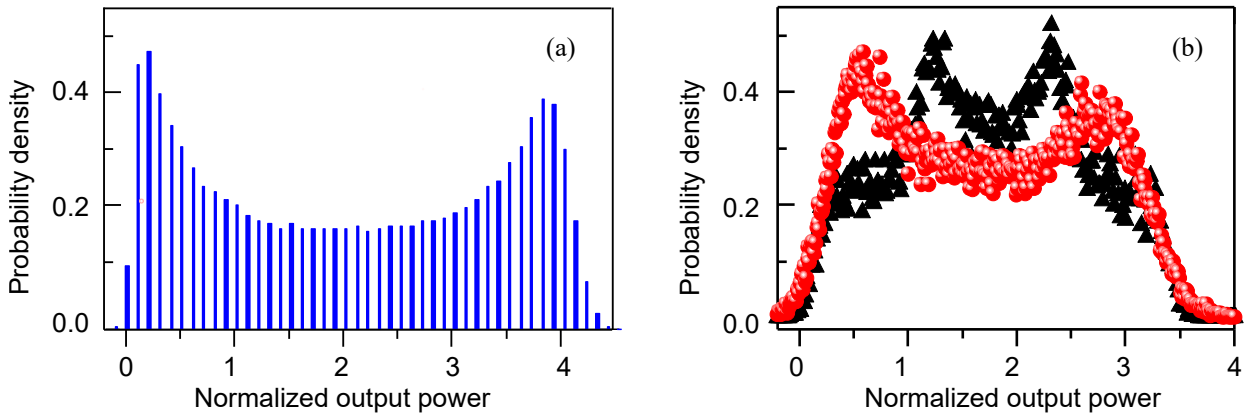


FIG. 2: Probability distribution for the interference: (a) modeling results for pulses with uniform relative phase and (b) real-life measurements [5].

By setting $f_p = 1/\Delta t$, one can thus make the first pulse interfere with the one following it. The light intensity at the photodetector can then be calculated as

$$I(t) = |E_1(t) + E_2(t)|^2, \tag{1}$$

where E_1 and E_2 are the laser field strengths of the two interfering laser pulses. These can be represented in the form

$$E(t) = A(t)\exp[i(\omega t + \varphi)], \tag{2}$$

where $A(t)$ is the pulse's envelope varying much slower than the field oscillation frequency $\omega = \frac{2\pi}{\lambda}c$. Substituting the field strengths (2) into (1) yields

$$I(t) = |A_1(t)\exp[i(\omega t + \varphi_1)] + A_2(t)\exp[i(\omega t + \varphi_2)]|^2 = A_1^2(t) + A_2^2(t) + 2A_1(t)A_2(t)\cos(\varphi_1 - \varphi_2). \tag{3}$$

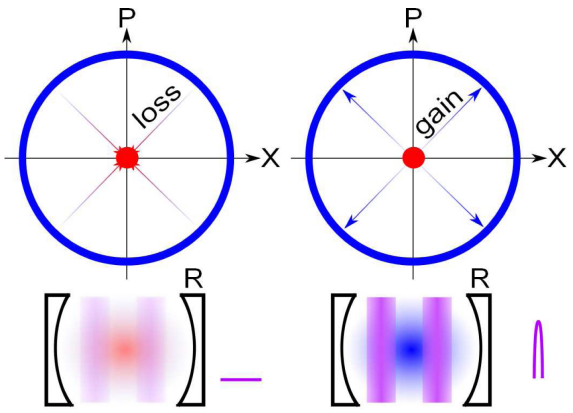
For the simplicity of the further derivations we will assume that the two pulses have identical shapes and amplitudes, i.e., $A_1(t) = A_2(t) = A_0$. Equation (3) then takes a shape of

$$\begin{gathered} I(t) = 2A_0^2(t)[1 + \cos(\varphi_1 - \varphi_2)] \\ \text{or} \\ \xi = \frac{I(t)}{A_0^2(t)} = 2(1 + \cos\Delta\varphi), \end{gathered} \tag{4}$$

where normalized intensity ξ ranges between 0 and 4 with respect to the relative phase $\Delta\varphi = \varphi_1 - \varphi_2$ of the laser pulses. With the latter quantity, the quantum randomness comes into play. The laser radiation arises from amplified spontaneous emission within the cavity, a process determined by the quantum fluctuations of the vacuum. It is this very phenomenon that gives a random nature to the phase of electric field within the pulse. If the two consecutive pulses arise from different photons, their phases are uncorrelated and uniformly distributed over $[0, \pi)$, and thus so is their difference, i.e., $\Delta\varphi \sim \mathcal{U}(0, \pi)$. It can then be shown that the probability distribution (or probability density function, PDF) of ξ is

$$F(\xi) = \frac{1}{2\pi}\frac{1}{\sqrt{1 - (0.5\xi - 1)^2}}, \xi \in [0; 4]. \tag{5}$$

This simple physical model describes theoretically ideal case. Real-world PDFs differ from it significantly due to practical imperfections of measurement equipment and finite coherence of laser pulses. Considering noises of the photodetector in the model gives PDF shown in Fig. 2a. Here, the singularities at the interval's end are damped, resulting in a bimodal and slightly broadened distribution. And Fig. 2b shows the experimental PDFs that are even worse compared to Fig. 2a. Moving of the peaks to the middle of PDF results from worse interference visibility owing to the next effects: chirp, jitter, and relaxation oscillations of laser pulses. Chirp is the frequency modulation of the pulse, jitter means fluctuations in pulse generation time, and the relaxation oscillation refers to small oscillations in which the laser power and laser gain are coupled to each other around their steady-state values. Their presence



(a) Loss mechanism scheme. **(b)** Gain mechanism scheme.

FIG. 3: Generation of amplified vacuum within the laser cavity. (a) The LD is first taken below threshold, to attenuate the cavity field to a weak thermal state (in red), independent of its previous value (in blue). (b) The LD is then taken above threshold, so that phase-insensitive amplification brings the field amplitude to a level fixed by saturation, while the phase retains the random thermal-state value [4].

is associated with laser dynamics and is intrinsically by nature when a semiconductor laser operates in a gain-switched mode. To improve interference visibility, some techniques are realized. For example, experimental PDFs of the interference signal in Fig. 2b are measured for the same pulse source without (filled triangles) and with (filled circles) dense-wavelength division multiplexing filter. Here, an optical filter improves spectral matching of the pulses improving thus their interference.

Knowing the practical PDF of intensity, one can then generate the random bit sequence in the following way:

1. Find the value I_{mid} that divides the distribution $F(I)$ into two parts of equal area under the curve.

2. Record the sequence of pulses from the interferometer, assigning the bit values according to the integral intensity I of each pulse in the following fashion

$$b = \begin{cases} 0, \text{ if } I \leq I_{mid} \\ 1, \text{ otherwise.} \end{cases} \tag{6}$$

Discussion of underlying quantum physics [4]. The method operates on the field within a single mode of a semiconductor diode laser. As shown in Fig. 3, the laser is first operated far below threshold, producing simultaneously strong attenuation of the cavity field and input of amplified spontaneous emission (ASE). This attenuates to a negligible level any prior coherence, while the ASE, itself a product of vacuum fluctuations, contributes a masking field with a true random phase. The laser is then briefly taken above threshold, to rapidly amplify the cavity field to a macroscopic level. Due to gain saturation, the resulting field has a predictable amplitude but a true random phase. The cycle is repeated, producing a stream of phase-randomized, nearly identical optical pulses. Interference of subsequent pulses converts the phase randomness into a stream of pulses with random energies that is directly detected and digitized.

E. Randomness extractor

Noise signal originating from quantum fluctuations is in principle unpredictable. However, in many applications, random numbers are required to be not only unpredictable but also **uniformly distributed**. However, raw bits from the digitized noise signal typically are non-uniformly distributed and thus cannot be directly used. To form a complete random number generation scheme, post-processing is required.

Randomness extraction is an essential process required to generate high-quality random numbers that are uncorrelated and uniformly distributed. The central part of the randomness extraction is usually an algorithm known as the randomness extractor. The randomness extractor receives a statistically weak binary stream as input, and generates uniformly distributed random bits at its output.

As an example, the earliest randomness extractor was Von Neumann extractor (Fig. 4). The algorithm receives the biased stream as input and divides the stream into pairs of bits. The output stream of such an algorithm is

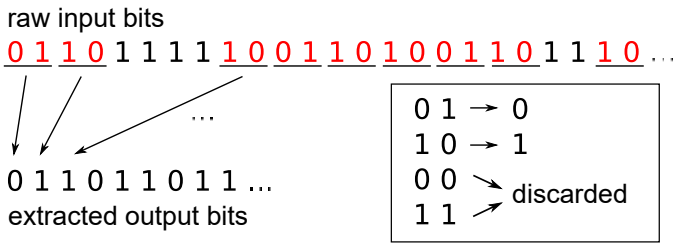


FIG. 4: Von Neumann randomness extractor. A stream of biased bits is divided into bit pairs. The algorithm discards all 00 and 11 pairs, and makes the mapping $01 \rightarrow 0$, $10 \rightarrow 1$. The resulted stream will have equal probability of 0s and 1s.

guaranteed to have uniform distribution between 0s and 1s. This extractor is only suitable for a biased stream of independent bits. If correlations exist between consecutive bits in the stream, this method is no longer applicable. Also, the algorithm is not considered efficient, as more than 75% of the bits from the input are lost while there is still entropy remaining available.

Many other implementations of randomness extractors have been reported, such as Trevisan's extractor [7], Toeplitz-hashing extractor, and random-matrix multiplication [8]. For implementations of random number generators, various families of cryptographic hashing functions are often adopted, such as secure hashing algorithms (SHAs) and advanced encryption standard (AES) hashing. These algorithms are usually carefully designed and have good performance. However, most cryptographic hashing functions are complicated and require lots of computational resources. This could be a limiting factor when one is pushing for a higher rate of random number generation.

F. Statistical test

Besides the generation of random numbers, it is also important to have ways of testing them. Lots of statistical tests have been created to assist the testing of random number generators. Some of the most famous test suites include NIST Statistical Test Suite and Diehard/Dieharder Suite by Robert G. Brown. Each of these test suites consists of dozens of carefully designed tests trying to probe possible statistical anomalies in the subjects, and they are often used to certify the performance of newly designed random number generators.

In this lab exercise, you will use NIST SP800-22 test suite "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications". It consists of 15 tests and explicitly defines recommendations and guidelines. Table I describes a bit sequence property that is verified with the corresponding NIST test [9, 10]. Each statistical test is formulated to test a specific null hypothesis (H_0). The null hypothesis under test is that the sequence being tested is random. Associated with this null hypothesis is the alternative hypothesis (H_a), which is that the sequence is not random. For each applied test, a decision or conclusion is derived that accepts or rejects the null hypothesis, i.e., whether the bit sequence is (or is not) random [10].

Each test is based on a calculated test statistic value, which is a function of the data. Then, it is used to calculate a P-value that summarizes the strength of the evidence against the null hypothesis. For these tests, each P-value is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of nonrandomness assessed by the test. If a P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A P-value of zero indicates that the sequence appears to be completely non-random. A significance level (α) can be chosen for the tests. If P-value $>= \alpha$, then the null hypothesis is accepted; i.e., the sequence appears to be random. If P-value $< \alpha$, then the null hypothesis is rejected; i.e., the sequence appears to be non-random. The parameter α denotes the probability of the error that the sequence produced by a truly random generator is evaluated as non-random (as it was discussed in the first section, even sequences of all 0s and 1s are equally probable as any other one sequence, and other patterns in the sequence might take place). Typically, α is chosen in the range $[0.001, 0.01]$.

Practically, NIST test uses 10^9 bit of random data to examine the distribution of the p-values, which are generated by repeating a test of 10^6 bit 1000 times. In this lab exercise, you will conduct tests only for a single bit sequence (of 30–65 kbit). The input data are regarded to be truly random if and only if they pass all the tests of NIST test suite.

TABLE I: NIST test names paired with descriptions. Adopted from [10].

Test Name	**Description**
Frequency	This test determines whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence (0s and 1s should each have a fraction of roughly 1/2).
Block Frequency	Tests that the proportion of zeroes and ones within M-bit blocks are close to $M/2$.
Runs	Tests whether the number of runs of ones and zeros of various lengths is as expected for a random sequence.
Longest Run	Tests sequence to determine if longest run is consistent with the length that would be expected in a random sequence.
Rank	This test checks for linear dependence among fixed length substrings of the original sequence.
FFT	Tests the spectral density of a sequence.
Non-overlapping Template	Tests the frequency of non-overlapping substrings.
Overlapping Template	Tests the frequency of overlapping substrings.
Maurer's Universal	Tests whether or not the sequence can be significantly compressed without loss of information. Too much compression indicates lack of randomness.
Cumulative Sums	Tests for deviations from the mean in the cumulative sum of the sequence.
Linear Complexity	Tests the complexity of a sequence, useful for detecting linear dependence which indicates non-randomness.
Serial	Tests whether the number of occurrences of the $2m$ m-bit overlapping patterns is approximately the same as would be expected for a random sequence.
Approximate Entropy	Compares the frequency of overlapping blocks of two consecutive/adjacent lengths (m and $m+1$) against the expected result for a random sequence.
Cumulative Sums	Determines whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences (bits are mapped to -1 and $+1$). If sums stray too far from zero is considered non-random.
Random Excursions	Determines if the number of visits to a state within a random walk exceeds what one would expect for a random sequence (bits are mapped to -1 and $+1$).
Random Excursions Variant	Detect deviations from the expected number of occurrences of various states in the random walk.

G. Entropy

Entropy in its many forms offers a convenient way to measure randomness. The different entropies give a mathematical measure for surprise (how unexpected a value is). We express entropy in bits, in the information-theory sense, which is closely related to the concept of thermodynamic entropy but takes it to a more natural formulation for information processing and communications.

Among possible methods of entropy estimation, in QRNG certification, the min-entropy is typically used. The min-entropy (in bits) of a random variable X is the largest value m having the property that each observation of X provides at least m bits of information (i.e., the min-entropy of X is the greatest lower bound for the information content of potential observations of X). The min-entropy of a random variable is a lower bound on its entropy. The precise formulation for min-entropy is $-log_2 \max p_i$ for a discrete distribution having n possible outputs with probabilities $p_1, \ldots, p_n$. Min-entropy is often used as a worst-case measure of the unpredictability of a random variable.

IV. EQUIPMENT

1. Educational fiber-optic scheme of Michelson interferometer made by RQC and QRate. It includes a distributed-feedback laser diode (DFB; Gooch & Housego AA1406) with a custom-made thermoelectric cooler (TEC) controller connected to it, fiber-optic circulator, fiber coupler 50:50, two Faraday mirrors, and a 25-m fiber patchcord.
2. Computer with data processing and testing software installed.
3. Signal pulse generator (Highland Technology P400).
4. Photodetector with 15 V AC adapter, pigtailed (Kongtum KT-PR-500M-A-FC-0, 500 MHz bandwidth).
5. Oscilloscope (LeCroy WavePro 735Zi or a similar model).
6. Fiber-coupled variable optical attenuator.
7. Fiber-optic patchcord FC/UPC-FC/UPC.
8. Cables and adapters (50 Ω coaxial cables LEMO 2 pcs., BNC-to-LEMO adapters 4 pcs., 50 Ω SMA to BNC coaxial cable).
9. Fiber-optic inspection microscope and cleaning kit.

Operator's manuals and data sheets for the equipment can be found on the course webpage.

V. WORKFLOW

The work proceeds in the following stages.

– Setting up QRNG scheme and data recording for two cases of QRNG operation: correct one and inappropriate one.

– Extracting a raw bit sequence from oscillograms (using a provided Python code).

– Applying NIST statistical tests (using a Python implementation of the testing algorithms).

– Preparing your report.

Operating and safety precautions

Do not apply the voltage to equipment, before lab assistant checks all the settings.

Warning

The TEC of LD should be powered on before all the other equipment! If you apply driving electric pulses to LD without operating TEC, it permanently damages the LD.

Before plugging the 5 V DC power supply into TEC, check its electrical polarity (power connector should be assembled according to keys "+" to "TIP").

Warning

Never apply voltage above 2 V to the oscilloscope input channel. The maximum input voltage of oscilloscope ProLink inputs with 50 Ω impedance is of ±2 V, while the electrical pulse generator has maximum voltage of 10 V. Be careful, verify that you apply lower voltage to oscilloscope channels.

1. **Setting up QRNG device**

   In this lab work, you will use a pre-assembled optical scheme of the unbalanced Michelson interferometer (see Fig. 1). To set up its operation as QRNG device, do the following steps.

   (a) Calculate pulse repetition rate for the Michelson interferometer to produce the interference of the first pulse with the second one.

   (b) **Power on the TEC of DFB laser using** 5 V **DC power supply.**

(a) (b)

FIG. 5: Oscilloscope settings. (a) Front panel controls. (b) Trigger dialog layout.

(c) In the channels' menu of the electrical pulse generator, set up the following settings.

Trigger: select *INTERNAL*, customize frequency according to calculation.

Channel to LD: set *POLARITY* +; VH +10.00; VL 0.00; *REL TO* T0; *WIDTH*: 5–10 ns.

Channel to oscilloscope: set *POLARITY* +; VH +1.00; *REL TO* T0; *WIDTH* is arbitrary.

Note: If you set too long pulses in the channel, the frequency decreases automatically. Verify before measurements that the frequency measured by the oscilloscope corresponds to the preinstalled value, within the accuracy of a quartz clock.

(d) Connect electrical pulse generator P400 output ports configured in the previous step to LD and to the oscilloscope, corresponding. The second electrical signal will be used for the triggering oscilloscope traces.

Note: for measurement of stable laser pulses, optical signal is traditionally used for triggering, but in the case of an interference signal, destructive interference will not trigger the measurement.

(e) Connect the oscilloscope to the optical scheme output via the photodiode (optical-to-electrical converter).

Here, you should take into consideration that the optical-to-electrical converter has a limited linear range. If its peak input optical power is too high, it will saturate and distort the pulse shape recorded at the oscilloscope. In the presence of saturation, the waveform peak becomes flat. To prevent saturation of a photodiode during this lab execution, follow the next instructions. Inset variable optical attenuator between the photodiode and optical scheme output, set its attenuation to 0 dB. Set PG frequency to distinguish optical pulses coming from the both interferometer arms and prevent their interference. Select attenuation value so that waveform peaks do not look flat or truncated. Gradually decrease attenuation until waveform starts to flatten, note this value of attenuation. Finally, set attenuation value at least 6 dB higher than the latter. If the variable optical attenuator is not available, you may introduce loss by separating fiber connectors slightly inside the bulkhead adapter, by unscrewing the connector's nuts and pulling them apart gently. The larger the gap between the connectors, the higher attenuation it introduces.

Another pitfall with this optical-to-electrical converter is that the oscilloscope software defaults on using a bandwidth-limiting filter ("reference receiver" in the probe configuration menu). If you want to see the real pulse shape at the full converter bandwidth, you must disable this filter in the configuration menu.

See the operator's manual for the converter if you have questions.

(f) Press the button *START* at the front panel of the pulse generator to apply electrical pulses to LD and oscilloscope.

Start oscilloscope in "Auto Trigger mode" by pressing "Auto" at the front panel [Fig. 5(a)]. It triggers the oscilloscope after a time-out, even if the trigger conditions are not met.

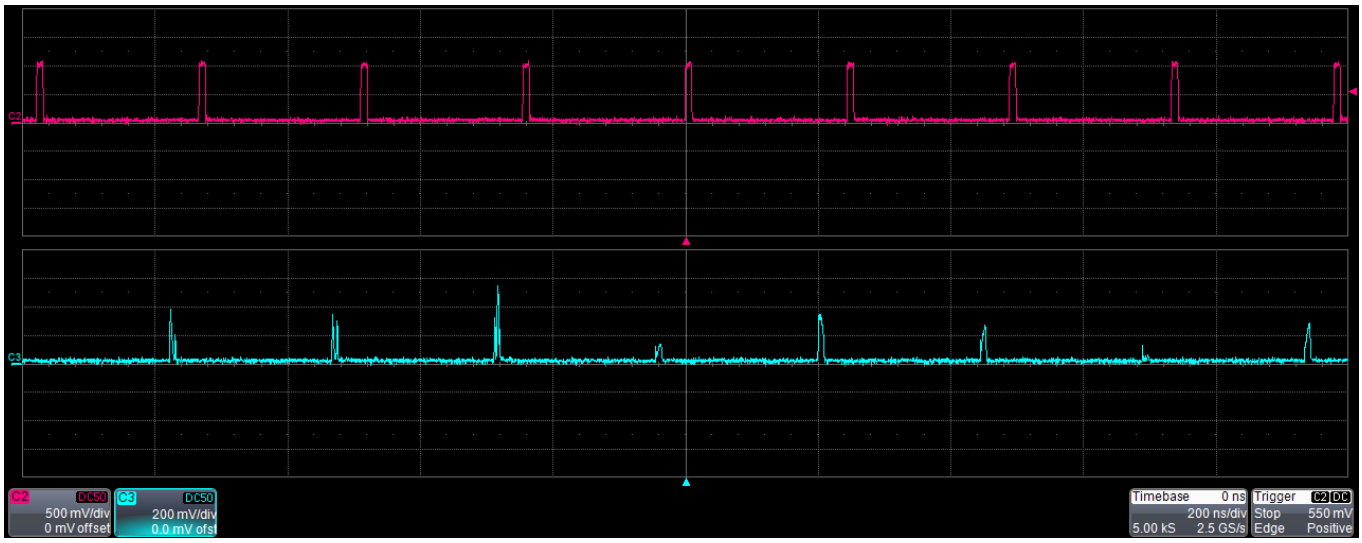


FIG. 6: An example of the oscilloscope screen with an oscillogram of synchronized electric channel (top trace) and interferometer output signal (bottom trace) with perfect time synchronization of interfering pulses.

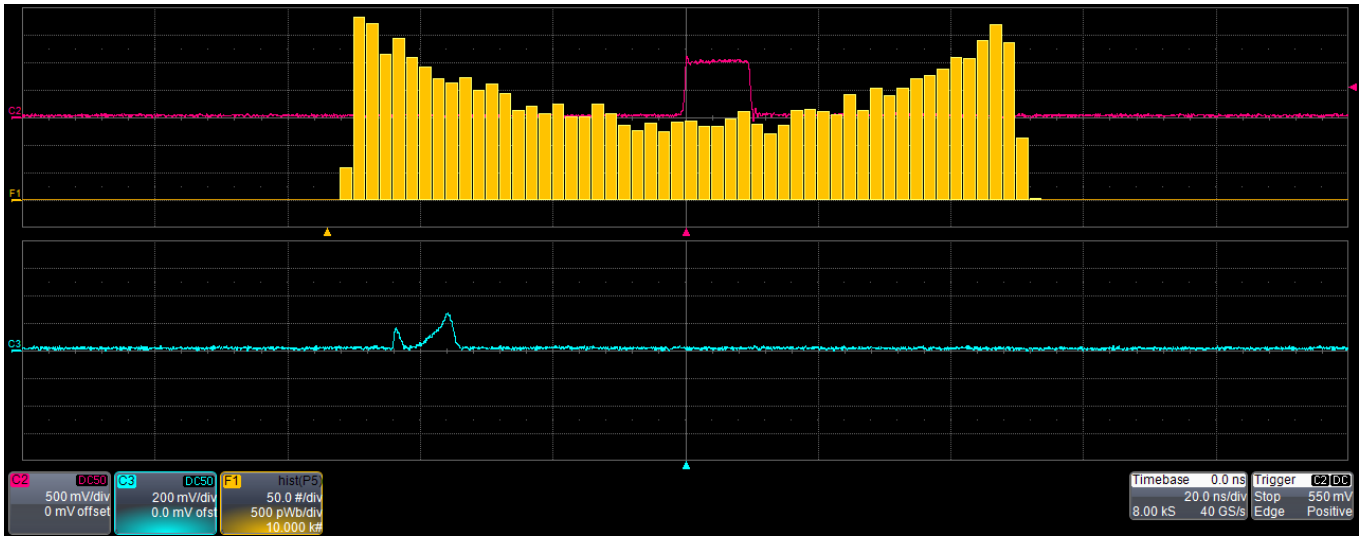


FIG. 7: An example of the oscilloscope screen with histogram on pulse area measurements corresponding to QRNG operation shown in Fig. 6.

In the oscilloscope settings, choose the channel where the PG electrical signal is connected as a trigger source. This is done in the following steps.

- To open trigger setup, press button “Setup” on the front control panel [Fig. 5(a)] of the oscilloscope.
- In the trigger dialog layout [Fig. 5(b)], press “Source” and select desired channel.
- In the trigger dialog layout [Fig. 5(b)], choose trigger type “Edge”, then adjust trigger threshold level by turning the knob “Level” at the front panel. The threshold level is indicated by the trigger label (the arrow on the right side of the oscillogram).

Set time and amplitude scales providing one interference pulse in the oscilloscope window. For ease of use, electrical and optical signals can be aligned relative to each other on the time axis by adjusting the delay in the settings of PG channels or using coaxial cables of different length.

(g) The real frequency (repetition rate) required to observe perfect interference differs a little bit from the calculated one. Now, you need to make a fine adjustment of the frequency by observing the measurement results on an oscilloscope. Figures 6 and 7 show oscilloscope screens with measurement results after fine adjustment of pulse generator frequency.

(a)

(b)

FIG. 8: Setting up histogram of area measurements. (a) Measurement dialog layout. (b) Histogram dialog layout.

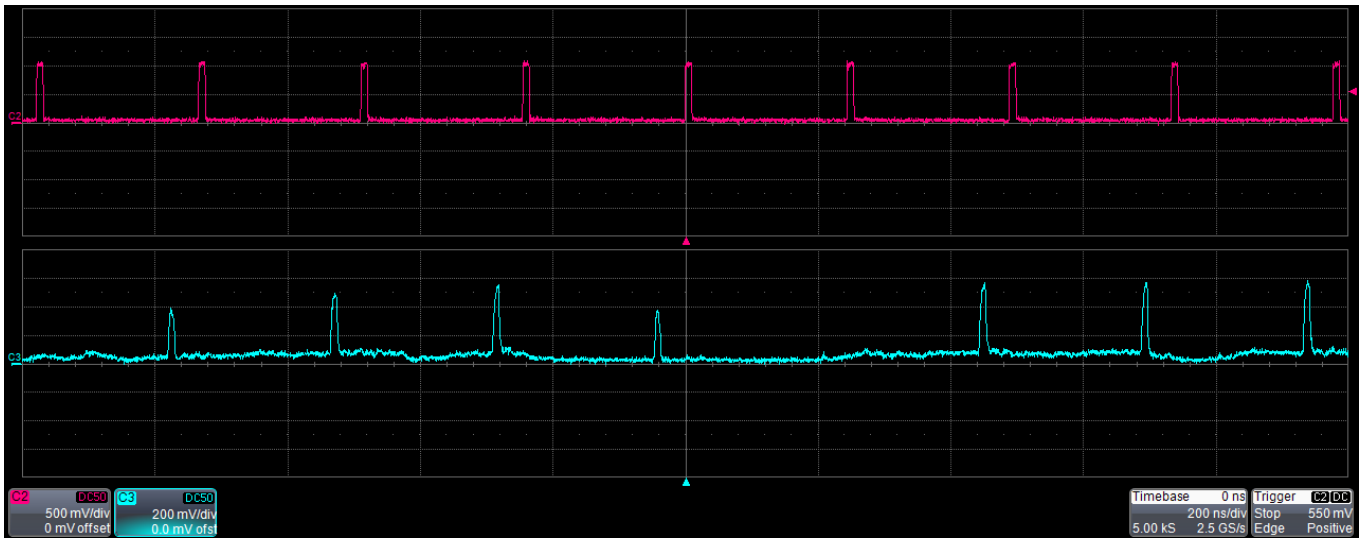


FIG. 9: An example of the oscilloscope screen with an oscillogram of synchronized electric channel (top trace) and interferometer output signal (bottom trace) with perfect time synchronization of interfering pulses. Bias of LD electrical pumping results in extended correlation time of pulses' phase.

In an oscillogram, you might observe narrow sub-pulses at the beginning of each signal pulse. It is caused by the absence of interference due to chirp, jitter, and relaxation oscillations, as described in [5].

(h) After fine adjustment, plot a histogram of area measurements. First, perform area measurements following next steps:

- Select " Measure" from the channel's shortcut toolbar buttons or from the top horizontal menu.
- In pop-up menu, choose "Area" (in category "Pulse"). Finally, set the measurement gate by tapping and dragging two vertical dashed lines in the channel layout. An example of area measurements with layout of measurement settings is in Fig. 8(a).

Finally, in the bottom menu of the measurement settings among layout "Actions for Px" choose "Histogram". In histogram dialog layout [Fig. 8(b)], set "#Values" of 1000–10000 and "#Bins" of 100–200. Save a histogram of area measurements.

(i) Measure and save a long pulse trace. In order to obtain a sufficient number of pulses, first, in the oscilloscope settings, reduce the sampling rate to 2.5 GS/s. Then extend the screen timescale as much as possible within the selected sampling rate.

(j) Finally, increase the low level of voltage applied to LD in the electrical pulse generator, VL, from 0 to 4 V. This should spoil interference statistics. On the oscilloscope, you will observe that the interference signal intensity tends to duplicate over several successive pulses, as shown in Fig. 9. Also you may notice in the oscillogram that some light appears in between the pulses. We recommend you to reduce the low voltage level to a point when this light all but disappears in the oscillogram, even if the pulses resume looking random at that point.

Save the data (histogram and a long pulse trace) as in the previous step.

Lab report should contain: diagram of your experimental setup, repetition rate calculation results, oscillograms presenting several interference pulses and histograms for pulse area measurements for both device settings, conditions of the measurements, and any observations and explanations you deem relevant.

2. **Extracting a raw bit sequence from oscillograms**

The Python implementation of a program to get a bit sequence imitates the measurement and processing parts of the QRNG device. Figure 10 explains its operation. First, it calculates an area of each signal pulse; then, it estimates a threshold value to divide the measurement events into two groups corresponding to bit values 0 and 1; and finally, it creates the bit sequence.

You should create two bit sequences, one for the proper operation and one for the incorrect operation of QRNG.

To process your oscillograms, follow these steps.

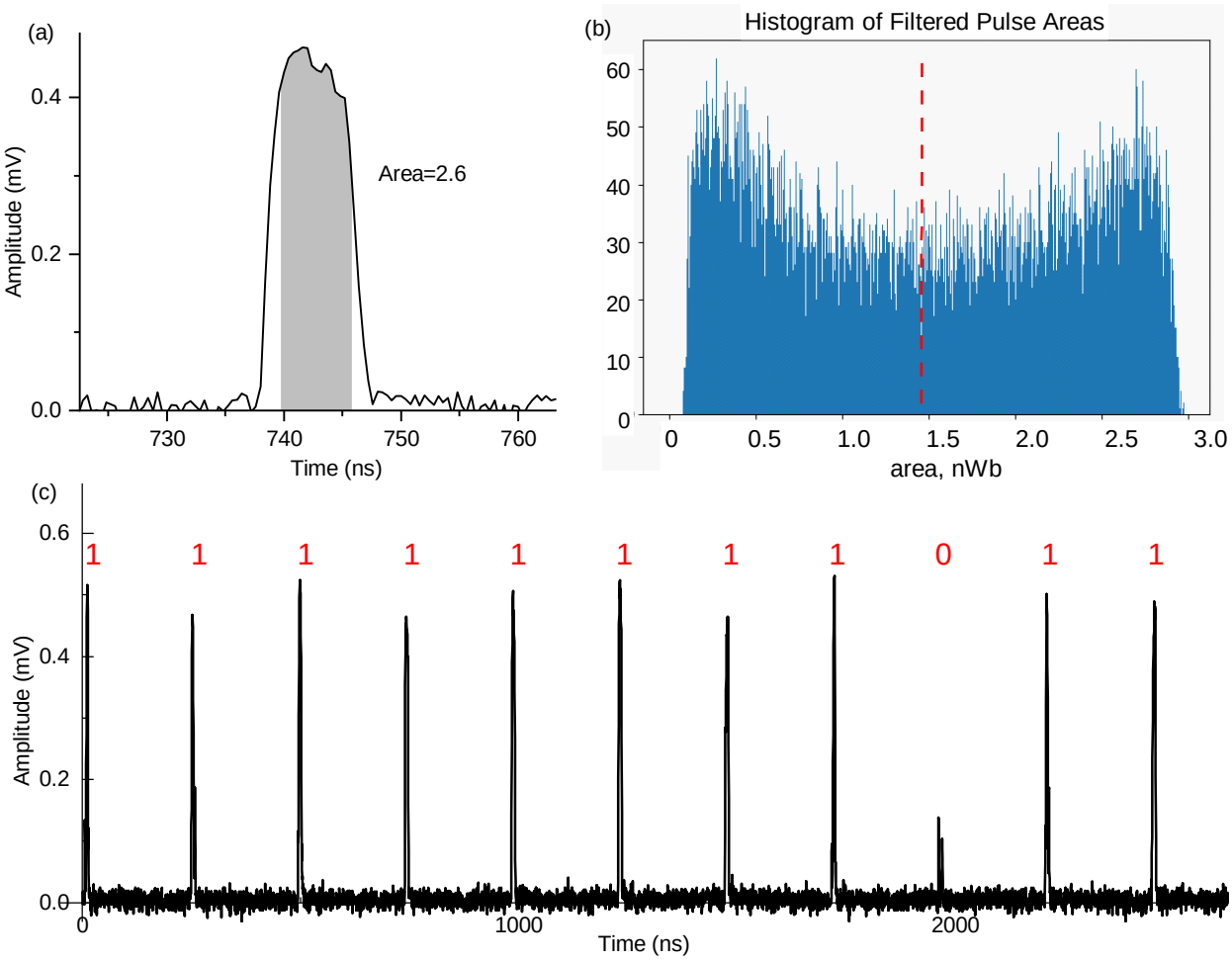


FIG. 10: Software simulator for measurement and it sequence production. (a) The program calculates area under each pulse according to selected time gate (selected pulse points). (b) It accumulates a probability density distribution of measurement events and estimates median area value (or threshold) that divides all the pulses into two groups, correspond to bit values 0 and 1. (c) Finally, the software produces the bit sequence from the oscillogram, based on calculated pulse areas using the estimated threshold level.

(a) Open and run the program QRNG-lab.py.

(b) Once you see the interface window (Fig. 11), choose "Select File" to upload oscillogram data (*.csv file) for processing or drag-and-drop it in the dialog window box. Next, press the button "Select Directory" and choose a folder where you want to save the processed data. In the dialog box, input the operating frequency of QRNG setup. Finally, clicking "Start Processing" starts the file handling.

(c) The next dialog window shows ten random pulses (Fig. 12). Firstly, you should check whether the pulses superimpose on one another. The pulses are scattered along the horizontal axis if you inserted an inaccurate signal repetition rate in the previous window. In this scenario, break the processing by clicking on the "Close" button and choosing "Exit" in the pop-up window.

In this window, you could set a time gate of pulses that will be used for the area calculation. To do that, you select pulse points by clicking on them with the left mouse button. The points of all plotted pulses at a chosen time will be colored in red. A second click with the left mouse button deselects the points and colors them in blue.

We recommend you to eliminate points at the beginning of pulses, where the interference is poor.

After finishing the time gate selection, click "Close" button and choose "Continue" in the pop-up window.

(d) Next, the program will show a window threshold level by which it divides the populations of measurements by two groups correspond to 0 and 1. Record the value, close the window.

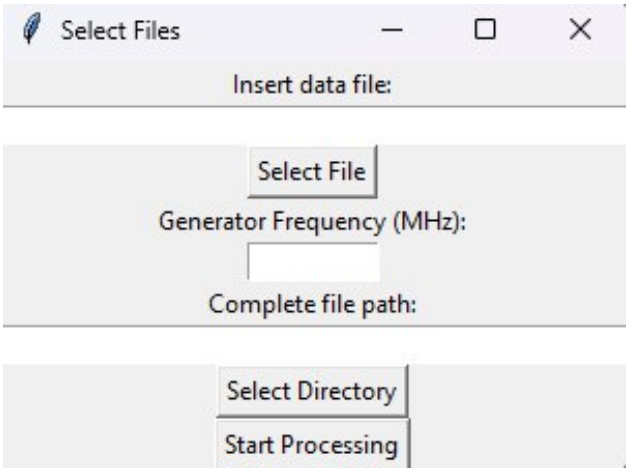
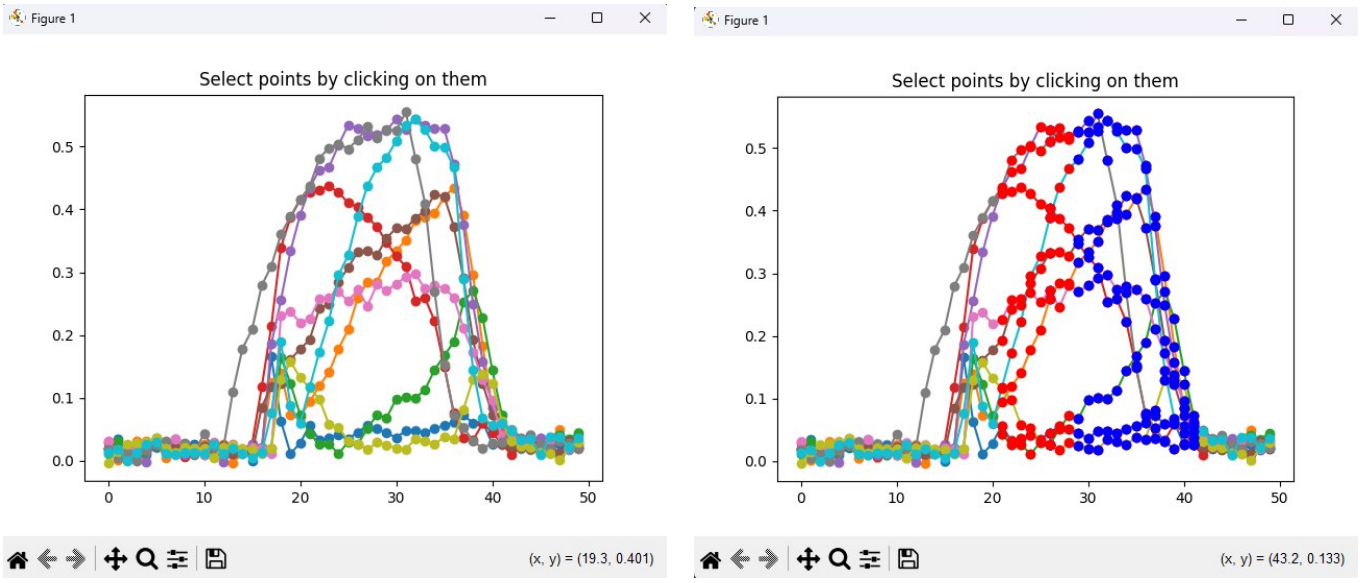


FIG. 11: Starting window of the program.



(a) (b)

FIG. 12: Window for selecting of time gate for calculations. (a) Initial view. (b) View after selecting/deselecting points for calculations.

(e) The next window shows histogram. Save it, close the window and wait for data saving. The saving finishes with a massage "Digitized pulses saved successfully".

3. **Make a randomness test of the obtained output data**

Use Python implementation of NIST's SP800-22 test suite.

(a) Open and run the program Main.py.

(b) Choose "Select Binary Data File" in "Input Data" box. This will open a file dialog where you should select the earlier prepared file with the bit sequence to be read by the program. The file should contain only one set of data in binary form.

(c) Run the test suite for both bit sequences. Record P-values, plot them, and compare the results.

(d) Explain the difference in test results for the correct and incorrect operation of QRNG.

Lab report should contain: P-values for correct and incorrect operation of QRNG device and discussion of the results.

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[2] V. L. Kurochkin, R. P. Ermakov, V. V. Zavodilenko, A. V. Losev, A. V. Udaltsov, V. V. Sharoglazova, R. A. Shakhovoy, and Y. V. Kurochkin, Attack-resistant quantum random number generator based on the interference of laser pulses with random phase (2021), U.S. patent no. US 11055404 B2.

[3] R. Shakhovoy, D. Sych, V. Sharoglazova, A. Udaltsov, A. Fedorov, and Y. Kurochkin, Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator, Opt. Express **28**, 6209 (2020).

[4] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Opt. Express **19**, 20665 (2011).

[5] R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference, IEEE J. Quantum Electron. **57**, 2000307 (2021).

[6] M. Petrov, I. Radchenko, D. Steiger, R. Renner, M. Troyer, and V. Makarov, Independent quality assessment of a commercial quantum random number generator, EPJ Quantum. Technol. **9**, 17 (2022).

[7] L. Trevisan, Extractors and pseudorandom generators, J. ACM **48**, 860 (2001).

[8] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, Quantum random number generation on a mobile phone, Phys. Rev. X **4**, 031056 (2014).

[9] C. Spear, D. Haycraft, L. Nguyen, H. Zhang, and Y. M. Sua, QCI's uniformly distributed quantum random number generator (uQRNG) (2023), `https://quantumcomputinginc.com/learn/module/introduction-to-uqrng/uqrng-whitepaper` [Accessed: (15 November 2024)].

[10] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22 (National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, 2010) `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf` .

Research Article | Vol. 28, No. 5 / 2 March 2020 / Optics Express 6209
Optics EXPRESS

Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator

ROMAN SHAKHOVOY,[1,2,*] DENIS SYCH,[1,2,3] VIOLETTA SHAROGLAZOVA,[1,2,4] ALEXANDER UDALTSOV,[1,2] ALEKSEY FEDOROV,[1,2,5] AND YURY KUROCHKIN[1,2,6]

[1]*Russian Quantum Center, 45 Skolkovskoye shosse, Moscow, Russia*
[2]*QRate, 100 Novaya str., Skolkovo, Russia*
[3]*P.N. Lebedev Physical Institute, Russian Academy of Sciences, 53 Leninsky prosp., Moscow, Russia*
[4]*Skolkovo Institute of Science and Technology, Bolshoy Boulevard 30, bld. 1, Moscow, Russia*
[5]*Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Russia*
[6]*NTI Center for Quantum Communications, National University of Science and Technology MISiS, 4 Leninsky prospekt, Moscow, Russia*
[*]*r.shakhovoy@goqrate.com*

Abstract: We propose a method for quantum noise extraction from the interference of laser pulses with random phase. Our technique is based on the calculation of a parameter, which we called the quantum reduction factor, and which allows for the determination of the contributions of quantum and classical noises with the assumption that classical fluctuations exhibit Gaussian distribution. To the best of our knowledge, the concept of quantum reduction factor is introduced for the first time. We use such an approach to implement the post-processing-free optical quantum random number generator with the random bit generation rate of 2 Gbps.

1. Introduction

Numerous quantum random number generators (QRNGs) based on various quantum effects have been demonstrated over the last two decades [1]. Among them, QRNGs employing different phenomena of quantum optics seem to be very convenient, relatively cheap, and, what is more important nowadays, could provide high random bit generation rates. Although optical QRNGs are extensively studied by many authors, the problem related to the contribution of classical noise in such QRNGs is still far from complete. This problem may seem overly pedantic at first glance. Perhaps for some scientific applications, such as Monte-Carlo simulations, it is. In cryptography, however, the extraction of purely quantum noise is crucial for secrecy and consequently is of fundamental importance.

Various approaches to evaluate the ratio between quantum and classical noises in optical QRNGs have been developed. Thus, in [2], where vacuum fluctuations were amplified using homodyne detection, the quantum noise contribution was estimated by calculating the difference between Shannon entropies of the amplified vacuum signal and the photodetector's dark signal. The SHA512 hash-function was then employed to extract quantum randomness from the raw bit sequence. A similar procedure for quantum noise extraction (but with other hash-function) was carried out in [3], where the interference of laser pulses with a random phase was proposed to generate random bits. For such a QRNG scheme, the same authors used later another approach [4], where the min-entropy of a random signal instead of the Shannon entropy was employed in the randomness extraction procedure. The same method to estimate the min-entropy was recently used in the optical QRNG of other authors [5], where the interference of pulses from a couple of gain-switched lasers was detected with balanced photodetector. To extract quantum

#380156 https://doi.org/10.1364/OE.380156
Journal © 2020 Received 6 Dec 2019; revised 3 Feb 2020; accepted 3 Feb 2020; published 19 Feb 2020

Optics EXPRESS

randomness, the authors used then Toeplitz extractor [6,7]. A more sophisticated approach of quantum noise extraction was used in [8,9], where random bits were generated by using the interference of a continuous-wave laser radiation in a Mach-Zehnder interferometer. Authors used the fact that according to [10,11] the quantum noise in their scheme is inversely proportional to the output laser power P. Recoding the dependence of the photodetector's voltage variance on P, they evaluated an optimal output laser power corresponding to the highest value of the quantum-to-classical noise ratio. The latter was then used to estimate the quantum min-entropy of the random signal needed for subsequent hashing.

An interesting method to make the correlated raw sequence uniform was proposed in [12], where authors used a finite-impulse response filter (FIR) to process the QRNG raw output. Such a filtering fuses bits of differing significances, thus achieving decorrelation of the raw data. Note, however, that such a processing is insecure in a cryptographic sense, since one can restore the raw sequence with all its inherent correlations, if the coefficients of the FIR filter are available. So, additional post-processing (i.e. randomness extraction) should be concatenated to the FIR, if such a QRNG is intended to use in cryptographic applications.

Another approach for data processing was proposed in [13], where a QRNG based on the interference of laser pulses was considered in the context of loophole-free Bell tests [14]. Authors considered the case of partially random bits in the output sequence and proposed the real-time method to increase its randomness. For this, neighboring bits were added modulo 2 recursively, i.e. the XOR operation was applied to the output sequence itself. The authors, however, noted that in case of completely predictable bits such an approach cannot be used. It is shown below that within our approach those bits that are related to the contribution of classical noise are (potentially) completely predictable; therefore, such a method is not applicable.

Obviously, there is no single rule to extract quantum noise from the output of the optical QRNG, particularly because the probability distribution of a random signal is highly dependent on the optical scheme. The quantum randomness extraction performed in [8] (and discussed later in detail by these authors in [7]) seems to be the most advanced approach to estimate quantum-to-classical noise ratio; however, this method is valid only when the interference term of the optical signal can be expanded into a series of the phase difference $\Delta\Phi$. In other words, such an approach can be applied only when the total phase fluctuations measured by the interferometric system are much less than unity, i.e., it is suitable only for the interferometers with sufficiently small time delay between the two arms [8]. Therefore, such method cannot be applied for the schemes with the interference of laser pulses with random phase [3–5], where $\Delta\Phi$ does not generally meet the requirement $\Delta\Phi << 1$. An attempt to extract quantum noise from the laser pulse interference was made in [4] (the same method was employed later in [5]); however, this approach seems to us not fully faithful, since it takes into account only the non-uniformity of the probability density function of the random signal, whereas the contribution of classical noise is not really taken into account. Moreover, it is not clear how to expand the proposed method for the case when a comparator is used to digitize a random signal instead of an analog-to-digital converter (ADC).

In the present work, we propose a different approach of the quantum randomness extraction for the optical QRNG based on the interference of laser pulses. Moreover, we propose a method to extract quantum noise without post-processing. In the next section, we provide some definitions that will be used across the paper. In section 3, we discuss main features of the interference signal and its probability distribution. In section 4, we discuss our method and introduce the so-called quantum reduction factor, which underlies the proposed approach. Finally, in section 5, we describe in detail the implementation of our QRNG.

Optics EXPRESS

2. Quantum vs classical randomness

Before discussing the problem of quantum randomness extraction, it is necessary to clarify what will we mean by randomness. Unfortunately, there is no widely accepted definition of random numbers. Just recall numerous definitions of random sequences given by D. Knuth [15] to realize the uncertainty surrounding this problem. Nevertheless, without giving definite conclusion, D. Knuth gives a recipe stating that a useful definition should contain a short list of properties desirable for random sequences. We will follow this recipe and formulate the basic requirements for random sequences in practical applications of our interest, namely in quantum key distribution (QKD).

The first requirement is that the random sequence should be *nondeterministic*. Obviously, pseudorandom number generators producing numerical sequences that appear "random", does not satisfy this requirement, since they represent computer algorithms, which are deterministic by definition. Consequently, this requirement forces the use of physical entropy sources. However, not any physical entropy source can be considered nondeterministic. Thus, fluctuations of the gas pressure are generally considered to be a stochastic process essentially because of its collective nature: it is almost impossible to predict an exact value of the gas pressure in every moment of time just because it is extremely difficult to solve differential equations and substitute in the general solution the initial conditions for the velocities and coordinates of all the particles of the gas. Nevertheless, such fluctuations are fundamentally deterministic in a sense that it is possible in principle to solve corresponding differential equations and find a precise value of the gas pressure in any moment of time. We will refer such fundamentally deterministic entropy sources to as *classical*. In contrast, electron tunneling through a potential barrier or spontaneous emission of an atom are fundamentally nondeterministic processes. In fact, one cannot find out the exact time when the electron tunnels through a barrier or when an atom spontaneously emits a photon. There is only a finite probability that after the measurement we will obtain a given result. We will refer the entropy sources based on such phenomena to as *quantum*, and only quantum entropy sources will be treated as nondeterministic.

The second requirement is that the entropy source should be fundamentally *uncontrollable* by the third party. This just means that the QRNG should be designed in such a way that an adversary was not able to influence the result of measurements made in the systems. If it is impossible to exclude completely an impact of an adversary, his influence should be taken into account, for instance, by the use of postprocessing.

The third requirement is that the physical process used in the QRNG should be *unpredictable*. It might seem at first glance that quantum nondeterministic phenomena are automatically unpredictable, and this requirement is redundant. However, the result of a quantum mechanical measurement is not necessarily unpredictable in the general case. For example, polarization measurements with a pair of entangled photons are 100% correlated, if both polarizers are aligned along the same axis. That is, each photon may be found randomly either in channel (+) or (–) of the corresponding polarizer, but when photon 1 is found positively polarized, then its twin companion 2 is also found positively polarized [16]. Such quantum correlations can potentially be used by an adversary to find out a secret key; therefore, by the source of quantum entropy we will hereinafter mean a system, in which there are no quantum correlations available for measurement by the third party.

Summarizing the above, we will refer the nondeterministic, uncontrollable and unpredictable noise to as *quantum noise*. The term *classical noise*, in turn, will be used with respect to fluctuations, which are fundamentally deterministic in nature and could be controlled or predicted by the third party.

Finally, let us make a remark regarding the term "truly random". In cryptography, one usually deals with uniformly distributed random bit sequences, so "truly random" usually means here "uniformly distributed" [17,18]. However, most physical entropy sources used to generate random

Optics EXPRESS

signals do not always allow directly obtaining uniformly distributed random bit sequences, since signal fluctuations are rarely exhibit a uniform probability density function (PDF). Therefore, in the context of physical RNGs, "truly random" usually means "not pseudorandom" regardless the form of its distribution. In the framework of the noise classification given above, we will use below the term "truly random" only with regard to quantum noise. Moreover, to satisfy cryptography requirements, we will assume that random bit sequences generated by a QRNG are also uniformly distributed. So, under "truly random" we will understand both "quantum" and "uniformly distributed".

3. Probability density function of the interference signal

The optical scheme of the QRNG under consideration allows transforming the laser phase fluctuations into amplitude fluctuations. For this, a continuous sequence of laser pulses is entered into an unbalanced interferometer, whose delay line is selected such that the corresponding delay time is a multiple of the pulse repetition period, so that pulses emitted by the laser at different moments of time are met at the output of the interferometer. An important requirement for the operation of this scheme is that the laser should be modulated over the lasing threshold, i.e., after each pulse the laser should be switched to the amplified spontaneous emission (ASE) mode [19,20]. Since most transitions in the ASE mode are spontaneous, phase correlations of the electromagnetic field are destroyed very quickly. As a result, each new laser pulse appears with a random phase; therefore, the result of the interference of two laser pulses will be a random quantity.

Let us make some remarks on the phase randomness in spontaneous emission process. It is well-known that spontaneous transitions are induced by zero-point oscillations of the electromagnetic field [21,22]. ASE could be thus treated as amplified vacuum fluctuations; therefore, some authors [3,4] use the relationship between vacuum fluctuations and spontaneous emission in order to attribute to latter the properties of vacuum, which is usually considered to be perfectly white, uncorrelated, and broadband. However, one should be careful when making such a generalization. In fact, perfect vacuum exhibit continuous set of states, whereas spontaneous emission in a laser is confined in its resonator with a finite number of modes, which changes the probability of spontaneous transitions [23]. Although individual spontaneous transitions are uncorrelated, correlation could exist between the phases of spontaneous emissions in a multilevel systems [24,25]. Fortunately, in semiconductor laser spontaneous emission is only correlated for a carrier scattering time that is of order 10^{-13} s, a negligibly short time; therefore, spontaneous emissions can be considered to obey Markovian assumption [11]. Due to this (and not just because of the relation to vacuum fluctuations), one can treat the laser phase noise as quantum noise.

Let us now turn to the question of the interference of laser pulses. Here, we will neglect the contribution of relaxation oscillations into the pulse shape and will assume that it exhibits the Gaussian temporal profile. Moreover, we assume that the light in the interfering pulses has the same polarization. With these assumptions, the integral intensity $\tilde{S}$ of the interference signal can be written as follows:

$$\tilde{S} = s_1 + s_2 + 2\eta\sqrt{s_1 s_2}\cos\Delta\Phi, \tag{1}$$

where s_1 and s_2 are normalized integral intensities corresponding to the optical output from the short and long arms of the interferometer, respectively, η is the visibility, and the phase difference is $\Delta\Phi = \Delta\varphi_p + \Delta\theta$. The phase difference $\Delta\theta$ is determined by the delay line ΔL and can be written as $\Delta\theta = k\Delta L n\omega_0/c$, where n is the refractive index of the optical fiber, ω_0 is the central frequency of the laser radiation, and the factor $k = 1, 2$ depends on the type of the interferometer (obviously, $k = 1$ if the Mach-Zehnder interferometer is used and $k = 2$ for the Michelson interferometer, since in this case the pulses pass the delay line twice). The phase difference $\Delta\varphi_p = \varphi_{p2} - \varphi_{p1}$, in turn, is determined by the initial phases of optical pulses at the laser output.

Optics EXPRESS

As discussed above, the phase of an optical pulse emitted by a gain-switched laser is assumed to be random. It should be noted here that such an assumption imposes some restrictions on laser operation, particularly on the pulse repetition rate ω_p and on the pump current amplitude I_p. In fact, at high ω_p the light coherence in the ASE mode could be destroyed incompletely [3,4], such that the phase of subsequent laser pulses will correlate. The gain-switched laser will require more and more pump current when increasing the modulation frequency, which makes high demands on a current pulse driver. Moreover, negative correlation can occur between laser intensity fluctuations for weak excitations [26]. So, one should select the optimal values of the pump current and the pulse repetition frequency to make the interference random. As an example, in [4] satisfactory randomness was achieved for $\omega_p / 2\pi = 5.825$ GHz with the reverse-biased distributed feedback (DFB) laser at $I_p \sim 100$ mA. Below, we assume that all parameters of the laser operation are set so that the randomness of the pulse phase is not disturbed. Particularly, the injection current of a laser is assumed to be always modulated over threshold with the modulation current amplitude not less than the threshold value. The pulse repetition period will be assumed to be always $\omega_p / 2\pi = 2.5$ GHz.

It was shown that phase fluctuations in the ASE mode are well described by the Langevin equations in terms of phase diffusion [11]. Langevin forces driving phase fluctuations can be shown to be nearly Gaussian, such that random phases of laser pulses φ_p can be assumed to be distributed according to the normal law with an rms of σ_φ. Obviously, the phase difference $\Delta\varphi_p$ between the two different laser pulses also has a normal PDF with an rms to be $\sigma_\varphi\sqrt{2}$. The same applies to the resulting phase difference $\Delta\Phi$ in Eq. (1). It can be shown (see Appendix) that if $\sigma_\varphi\sqrt{2} > 2\pi$ the PDF of the resulting phase $\Delta\Phi$ can be defined with high accuracy by

$$f_{\Delta\Phi} = \begin{cases} \frac{1}{\pi}, & \Delta\Phi \in [0, \pi) \\ 0, & \Delta\Phi \notin [0, \pi) \end{cases}. \tag{2}$$

It should be noted that $\Delta\Phi$ could fluctuate under the influence of both quantum and classical noises. However, due to the fact that $\Delta\Phi$ is in the argument of the cosine (Eq. (1)), the influence of the classical component will be completely overlapped by quantum noise, if the rms of the quantum noise component is greater than 2π. Indeed, the PDF of $\Delta\Phi$ in this case can be considered uniform within $[0, \pi)$ regardless the amount of the classical noise component. Hereinafter, we assume that the rms of the laser phase diffusion obeys the inequality $\sqrt{2}\sigma_\varphi > 2\pi$, such that $f_{\Delta\Phi}$ can be defined by Eq. (2) and fluctuations of $\Delta\Phi$ can be thus treated as truly random.

If $\Delta\Phi$ is distributed according to Eq. (2), whereas s_1, s_2 and η are assumed to be constant, then the PDF of the integral signal $\tilde{S}$ is defined by the derivative: $f^Q_{\tilde{S}} = (F^Q_{\tilde{S}})'$, where, by definition, the cumulative distribution function (CDF) $F^Q_{\tilde{S}}$ is given by [27]:

$$F^Q_{\tilde{S}}(y) = \int\limits_{\tilde{S} < y} f_{\Delta\Phi}(x)dx, \tag{3}$$

where x stands for the value of $\Delta\Phi$ and the integration region is given by the inequality $s_1 + s_2 + 2\kappa\sqrt{s_1 s_2}\cos x < y$. Substituting Eq. (2) into Eq. (3) we obtain

$$f^Q_{\tilde{S}}(x) = \left[\pi\sqrt{(x - \tilde{S}_{min})(\tilde{S}_{max} - x)}\right]^{-1}, \tag{4}$$

where

$$\begin{aligned} \tilde{S}_{min} &= s_1 + s_2 - 2\eta\sqrt{s_1 s_2}, \\ \tilde{S}_{max} &= s_1 + s_2 + 2\eta\sqrt{s_1 s_2}. \end{aligned} \tag{5}$$

Optics EXPRESS

We will refer the function $f^{Q}_{\tilde{S}}(x)$ given by Eq. (4) to as a *quantum* PDF of the interference signal, since it is defined solely by fluctuations of $\Delta\Phi$, which we agreed to consider quantum. The function $f^{Q}_{\tilde{S}}(x)$ for the case $s_1 = s_2 = 1$ at different values of visibility η is shown in Fig. 1(a). One can see that $f^{Q}_{\tilde{S}}(x)$ tends asymptotically to infinity for ideal destructive ($x = \tilde{S}_{min}$) and constructive ($x = \tilde{S}_{max}$) interference. The "distance" between the asymptotes

$$\tilde{S}_{max} - \tilde{S}_{min} \equiv w_{\Delta\Phi} = 4\eta\sqrt{s_1 s_2}, \tag{6}$$

we will refer to as the width of the quantum distribution. One can see from Fig. 1 and Eq. (6) that $w_{\Delta\Phi}$ is decreased when decreasing η.

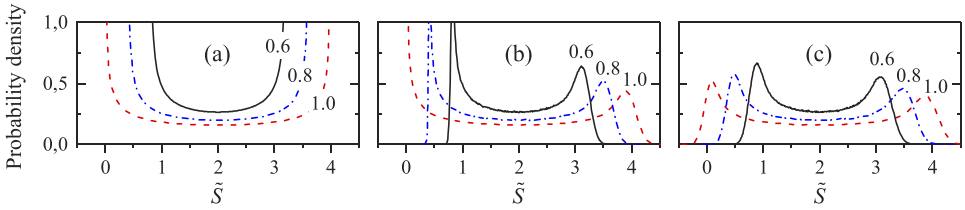


Fig. 1. (a) Quantum PDF of the interference signal (Eq. (4)) for three different values of the visibility η (0.6, 0.8, and 1). (b) Monte-Carlo simulations of the signal PDF in the presence of fluctuation of s_1 and s_2 in Eq. (1). (c) Monte-Carlo simulations of the signal PDF in the presence of fluctuation of s_1 and s_2 and the photodetector's noise as well.

In addition to fluctuations of $\Delta\Phi$ one should take into account fluctuations of s_1 and s_2. The CDF of the interference signal should be then rewritten as follows

$$F_{\tilde{S}}(y) = \int\limits_{\tilde{S} < y} f_{\Delta\Phi}(x_1) f_{s_1}(x_2) f_{s_2}(x_3) dx_1 dx_2 dx_3, \tag{7}$$

where the values of random variables $\Delta\Phi$, s_1 and s_2 are denoted by x_1, x_2, and x_3, respectively, and where it is assumed that fluctuations of $\Delta\Phi$, s_1 and s_2 are independent, such that the joint PDF represents just a product of all corresponding PDFs: $f_{\Delta\Phi} f_{s_1} f_{s_2}$. The integration area is defined now by the inequality $x_2 + x_3 + 2\eta\sqrt{x_2 x_3}\cos x_1 < y$. Note also that fluctuations of η are neglected in Eq. (7). Finally, the resulting PDF of the interference signal is determined by a derivative of the CDF: $f_{\tilde{S}} = F'_{\tilde{S}}$. Unfortunately, the integral in Eq. (7) cannot be calculated analytically; therefore, Monte Carlo simulations are usually used to find $f_{\tilde{S}}$.

It seems reasonable to consider fluctuations of s_1 and s_2 as a Gaussian noise. Since this noise is related to the pump current fluctuations, it should be referred to as classical. Monte-Carlo simulations for the case when f_{s_1} and f_{s_2} are Gaussian with $\bar{s}_1 = \bar{s}_2 = 1$, whereas $f_{\Delta\Phi}$ is defined by Eq. (2), are shown in Fig. 1(b). One can see from the figure that the PDF exhibits noticeable asymmetry: the left maximum is much higher and "thinner" than the right one. This feature is due to fluctuations of normalized amplitudes s_1 and s_2 and it becomes more pronounced when increasing the rms value of these fluctuations. Note that the normalized rms value of the output laser power fluctuations σ_s was usually measured to be 4-6% of the pulse average power, so the value $\sigma_{s_1} = \sigma_{s_2} = 0.05$ was used in simulations shown in Figs. 1(b,c).

In a real experiment, the PDF of the interference signal is additionally "broadened" due to noises in the photodetector. An experimental signal should be thus written in the following form:

$$\tilde{S} \to \tilde{S} + \zeta, \tag{8}$$

where ζ is the photodetector's Gaussian classical noise. Simulations of $f_{\tilde{S}}$ in the presence of fluctuations of s_1, s_2 and the photodetector's noise as well (the rms of the photodetector noise was put to $\sigma_\zeta = 0.1$) are shown in Fig. 1(c).

Optics EXPRESS

It should be noted that the laser pulse interference could have another features, which adversely affect the visibility and have an impact on the appearance of the PDF of the random interference signal. Thus, we did not yet consider the influence of chirp and jitter, whose combined effect in the context of QRNG was considered in [12], where authors demonstrated that the PDF of the interference signal for chirped laser pulses differs markedly from the PDF measured in the absence of chirp. It is well-known that Gaussian laser pulses exhibit linear chirp [19], such that the time dependence of the electric field of the pulse is proportional to $\exp[i(\omega_0 t - \beta t^2)]$, where ω_0 is the central frequency of the laser field and the linear chirp coefficient is $\beta = \alpha / 2w^2$, where w is the rms width of the laser pulse and α is the linewidth enhancement factor (the Henry factor [10]). The visibility of the integrated interference signal in Eq. (1) is now defined by [28]

$$\eta = e^{-\frac{(1+\alpha^2)\Delta t^2}{8w^2}}, \tag{9}$$

where Δt is the inaccuracy of pulse overlap, which fluctuates due to jitter. Therefore, Eq. (7) should be supplemented by the jitter PDF $f_{\Delta t}$, which is usually assumed to be Gaussian.

Monte-Carlo simulations of $f_{\tilde{S}}$ taking into account the influence of the "linear chirp + jitter" effect are shown in Fig. 2. For simulations, we used Eq. (1) with the visibility η defined by Eq. (9), where we put $\alpha = 6$ and $w = 50$ ps. Fluctuations of s_1 and s_2 were again assumed to be Gaussian with $\bar{s}_1 = \bar{s}_2 = 1$ and $\sigma_{s_1} = \sigma_{s_2} = 0.05$, $f_{\Delta\Phi}$ was defined by Eq. (2) and the photodetector noise was introduced according to Eq. (8) with $\sigma_\zeta = 0.1$. The jitter was assumed to exhibit Gaussian PDF with the rms from 0 to 20 ps and with mean value equal to zero. One can see that the jitter with $\sigma_{\Delta t} > 10$ ps markedly affects the form of the signal PDF leading to the appearance of the central peak, which indicates an increase in the probability that the signal equals to $\tilde{S} = s_1 + s_2$, which is the evidence of interference worsening. However, at small $\sigma_{\Delta t}$ (or, equivalently, at small α) the influence of the "linear chirp + jitter" effect on the PDF is insignificant (compare PDFs on Fig. 2 at $\sigma_{\Delta t} = 0$ and $\sigma_{\Delta t} = 5$ ps), such that one can neglect it. Moreover, the "linear chirp + jitter" effect can be reduced by cutting off the high-frequency and low-frequency parts of the laser spectrum with the bandpass filter. This is the consequence of the fact that the spectrum of the chirped Gaussian laser pulse exhibits inhomogeneous broadening in addition to broadening associated with a finite pulse duration. The spectral filtering changes the intensity distribution of spectral components in the pulse making it effectively less chirped.

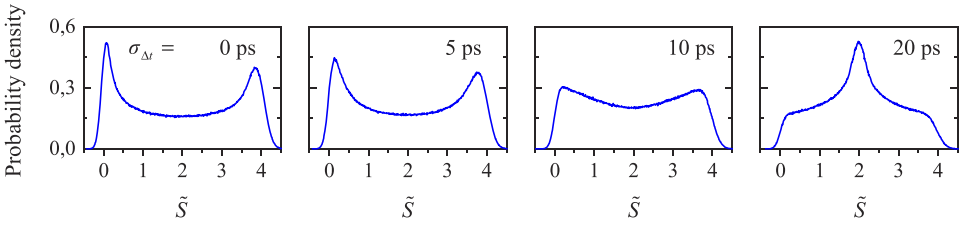


Fig. 2. Monte-Carlo simulations of the signal PDF taking into account the influence of the "linear chirp + jitter" effect. The values of the jitter rms are shown on the corresponding simulations.

A more complicated picture takes place when the laser pulse is distorted by relaxation oscillations, since the chirp is not linear in this case. A more detailed study of this issue, particularly the influence of chirp, jitter and relaxation oscillations on laser pulse interference we consider elsewhere [29], showing that the combined effect of chirp and jitter can be decreased even in this case by cutting off only the high-frequency part of the laser spectrum with the bandpass filter. Thus, we will assume below that the "chirp + jitter" effect is decreased to be small enough, such that the visibility η is not significantly changed from one pair of pulses to another and we can treat it as a non-fluctuating parameter.

Optics EXPRESS

The key to separate quantum and classical noises is the comparison of functions $f_{\tilde{S}}$ and $f_{\tilde{S}}^{Q}$. Obviously, the more these functions are different from each other, the greater the contribution of classical fluctuations. In the next section, we describe a method to calculate the so-called quantum reduction factor, which in a sense determines the quantum-to-classical noise ratio in the assumption of Gaussian classical noises. As the main sources of classical noise, we will consider the photodetector noise and fluctuations of the laser output power (the latter correspond to fluctuations of quantities s_1 and s_2). In view of the above, fluctuations of the visibility η and corresponding impact of jitter will be neglected. We will further restrict our consideration to the case when an adversary can influence only the part of the classical noise, which is related to the photodetector. It means that if the magnitude of the classical noise in the QRNG system varies with time, this variation can be mainly attributed to the photodetector and a possible influence of an attacker on it. This does not mean, however, that under this assumption we exclude from consideration another part of the classical noise related to fluctuations of the laser output power. The latter will still be included in the model by Eq. (7) and thus will make its impact into the quantum reduction factor. The only assumption is that the magnitude of this part of the classical noise, i.e. the values of σ_{s_1}, σ_{s_2}, will be assumed to be fixed.

4. Quantum reduction factor

As we mentioned in the Introduction, quantum and classical noises can be "separated" at the post-processing stage. In fact, it can be formally assumed that the output random sequence may contain correlations associated not only with non-uniformity of the digitized signal, but also with the contribution from the classical noise. This means that the randomness extraction (RE) procedure should be carried out taking into account the ratio between quantum and classical noises.

The RE procedure can be considered as some operation that transforms a binary sequence $\{0,1\}^l$ of length l with *non-uniform* distribution of elements into a binary sequence $\{0,1\}^m$ of length m, where distribution of elements is *close to uniform*. The length of the binary sequence with improved randomness is generally shorter: $m < l$. With such a definition, the RE procedure can be treated as a reduction of a raw random bit sequence: $\{0,1\}^l \xrightarrow{\text{RE}} \{0,1\}^m$, and a ratio $\gamma = l/m$ is sometimes referred to as a reduction factor. In conventional RE procedures, the reduction factor γ is estimated via the min-entropy H_∞ of the raw sequence. Thus, a perfect randomness extractor applied to a non-uniform random sequence $\{X_1, X_2, \ldots, X_N\}$ with $N >> 1$, where each X_i is an n-bit word, could provide NH_∞ almost uniformly distributed bits [17], i.e. the raw sequence will be reduced with such an extractor by a factor of $\gamma = nN/NH_\infty = n/H_\infty$. The min-entropy, in turn, is defined as $H_\infty = -\log_2 p_{max}$, where p_{max} is the highest probability to guess a random element from the sequence $\{X_1, X_2, \ldots, X_N\}$. If the random signal is digitized by an ADC, then n in the definition of γ corresponds to the resolution of the ADC in bits, whereas p_{max} corresponds to the probability of the most likely bin. If the digitization is performed using a comparator ($n = 1$), then the reduction factor is determined as $\gamma = 1/H_\infty$. If, in addition, the comparator threshold is chosen such that probabilities of '1's and '0's in the QRNG's output are equal, then $H_\infty = 1$ and the reduction factor is $\gamma = 1$, i.e., a raw random sequence could be employed. Obviously, such a result contradicts physical considerations, since the classical noise introduced by the photodetector and other devices included in the QRNG cannot be generally neglected, so the raw random bit sequence should be subject to reduction anyway. Therefore, the reduction factor should be redefined to take into account classical noises.

It seems that there is no universal way to estimate contributions of classical and quantum noises to laser pulse interference. One can see from Fig. 2 that the "chirp + jitter" effect complicates the appearance of the signal PDF and it is not obvious how to compare functions $f_{\tilde{S}}$ and $f_{\tilde{S}}^{Q}$, when $f_{\tilde{S}}$ exhibit significant central peak (see Fig. 2 on the right). As we already agreed, we will neglect the influence of the "chirp + jitter" effect on the signal PDF and will consider the photodetector noise

Optics EXPRESS

and fluctuations of the laser output power as the main sources of the classical noise. Assuming further that the interference signal is digitized with the comparator, we can quite easily estimate the contribution of classical fluctuations.

One can see from Fig. 1 that the Gaussian noise broadens the PDF of the interference signal, such that the probability for the signal to fall in the region between $\tilde{S}_{min}$ and $\tilde{S}_{max}$ decreases when increasing the rms of the photodetector noise. We can thus say that an additional classical entropy "flows" into the $[\tilde{S}_{min}, \tilde{S}_{max}]$ interval. Let us agree that if the contributions of classical and quantum noises are equal in this interval, we will not trust the resulting random sequence at all (even if it passes all randomness tests!) and require the reduction factor to be made infinitely large. (We will discuss such an assumption below.) In contrast, if the contribution of classical noises is negligibly small, then the reduction factor can be put to unity (note that this assumption is valid only for the case of a comparator with a properly chosen threshold). Such a reduction factor that takes into account the contribution of classical noise and allows extracting pure quantum randomness we will refer to as a *quantum reduction factor* Γ. Let us now find the relation between Γ and the min-entropy.

In the ideal case, when the classical contribution is absent, the comparator threshold voltage (or rather its normalized value) should be obviously set to $V_{th} = \tilde{S}_{min} + w_{\Delta\Phi}/2$, and the min-entropy can be written as follows:

$$H_\infty^Q = -\log_2\left(\int_{\tilde{S}_{min}}^{\tilde{S}_{min}+w_{\Delta\Phi}/2} f_{\tilde{S}}^Q(x)dx\right) = 1, \tag{10}$$

where the integral in parentheses corresponds obviously to p_{max}. We will refer H_∞^Q to as a quantum min-entropy. The min-entropy in the presence of classical noise we define in a similar way:

$$H_\infty = -\log_2\left(\int_{\tilde{S}_{min}}^{\tilde{S}_{min}+w_{\Delta\Phi}/2} f_{\tilde{S}}(x)dx\right) \geq 1. \tag{11}$$

Following the above agreement, we will assume that if H_∞ is twice H_∞^Q, then $\Gamma \to \infty$. If, however, $H_\infty \to H_\infty^Q$, then $\Gamma \to \gamma = 1/H_\infty$. Obviously, both requirements are satisfied, if the quantum reduction factor is defined as follows:

$$\Gamma = \frac{1}{2 - H_\infty}. \tag{12}$$

It is obvious from the above that $H_\infty \geq H_\infty^Q$ and, consequently, $\Gamma \geq \gamma$, and the equality holds in the absence of classical noises. Thereby, the reduction factor γ determines the non-uniformity degree of a random sequence, but it does not take into account the contribution of classical noise. The quantum reduction factor Γ, in turn, takes into account both effects and thus allows estimating the length of the random bit sequence returned by the RE algorithm, which will be guaranteed to have a quantum nature.

The theoretical dependence of the quantum reduction factor Γ on the photodetector noise rms σ_ζ is shown in Fig. 2(a) on the left. The simulations of the integral interference signal $\tilde{S}$ PDF corresponding to three different values of σ_ζ are shown on the right. It was assumed in the simulations that the photodetector noise is included in $\tilde{S}$ according to Eq. (8); the fluctuations of s_1 and s_2 were again assumed to be Gaussian with $\bar{s}_1 = \bar{s}_2 = 1$ and $\sigma_{s_1} = \sigma_{s_2} = 0.05$. The selected points on the curve $\Gamma(\sigma_\zeta)$ are connected by arrows with the corresponding theoretical PDFs. One can see that Γ grows with the growth of σ_ζ, since the proportion of the noise, which may be compromised by the adversary, increases.

Optics EXPRESS

One should remember that Γ depends also on σ_{s_1} and σ_{s_2}, which are assumed to be fixed in the present consideration. Assuming that $\sigma_{s_1} = \sigma_{s_2} = \sigma_s$ we may write for a more general case $\Gamma = \Gamma(\sigma_\zeta, \sigma_s)$, such that the quantum reduction factor can be presented as a 2D surface or as a set of $\Gamma(\sigma_\zeta)$ curves corresponding to different magnitudes of laser pulse fluctuations. We will not consider this case here.

There is a certain arbitrariness in the definition of the quantum reduction factor given by Eq. (12). In fact, we demand that Γ should be put to infinity when the contributions of classical and quantum noises are the same. Probably, such a requirement is overly rigid, but it guarantees that the random sequence resulting from the RE procedure with such a reduction factor will indeed have a quantum nature. We use the min-entropy as a measure to compare quantum and classical noises not only because H_∞ is used in the definition of γ, but also because such a choice seems very natural. Indeed, we do not trust the noise, if the probability for the signal $\tilde{S}$ to fall into the interval from $\tilde{S}_{min}$ to $w_{\Delta\Theta}/2$ is changed from $1/2$ to $1/4$, i.e. when the min-entropy doubles. In this case, the probability of a '0' or '1' is equally related to both quantum and classical effects, i.e. quantum and classical noises become in a sense indistinguishable.

This interpretation can be expanded for the case $n > 1$, i.e. when an ADC is used for the digitization. Let us again require the quantum reduction factor to become infinitely large when the probability p_{max} of the most likely bin is halved due to classical noise contribution. We define this probability now as follows:

$$p_{max} = \int_{\tilde{S}_{min}}^{\tilde{S}_{min}+\Delta u} f_{\tilde{S}}^{Q}(x)dx, \tag{13}$$

with the bin size $\Delta u = \Delta U/2^n$, where ΔU is the dynamic range of the ADC, and where we use the fact that $f_{\tilde{S}}^{Q}(x)$ behaves asymptotically near $\tilde{S}_{min}$. The quantum min-entropy is obviously defined as $H_\infty^Q = -\log_2 p_{max}$, whereas the value of the min-entropy, at which $\Gamma \to \infty$, is $-\log_2(p_{max}/2) = 1 + H_\infty^Q$. So, we can define the quantum reduction factor as follows:

$$\Gamma = \frac{n}{1 + H_\infty^Q - H_\infty}, \tag{14}$$

where similar to Eq. (11)

$$H_\infty = -\log_2\left(\int_{\tilde{S}_{min}}^{\tilde{S}_{min}+\Delta u} f_{\tilde{S}}(x)dx\right) \tag{15}$$

and H_∞^Q is defined accordingly, but with $f_{\tilde{S}}^{Q}$ in the integral. One can see that with such a definition Eq. (12) becomes an extreme case of Eq. (14) at $n = 1$, if Δu is treated as $w_{\Delta\Phi}/2$.

5. QRNG implementation

The schematic diagram of our QRNG is shown in Fig. 3(a). The optical scheme depicted by the dashed rectangle includes generally two principal elements: the fiber optic interferometer (it is an unbalanced Michelson interferometer in our case) and the photodetector. Note that the optical scheme in Fig. 3(a) may generally refer to any scheme that allows implementing the interference of laser pulses. Optical pulses are generated by the distributed feedback laser modulated over threshold with the frequency 2.5 GHz by a laser diode driver. To digitize the photodetector signal we propose to use the set of three high-speed comparators. The comparator C0 is needed to find the PDF of the interference signal, whereas the comparators C1 and C2 work in parallel acquiring the signal from the photodetector and providing the digital output. Obtained random bits are received by the field-programmable gate array (FPGA) for buffering and further processing.

Optics EXPRESS

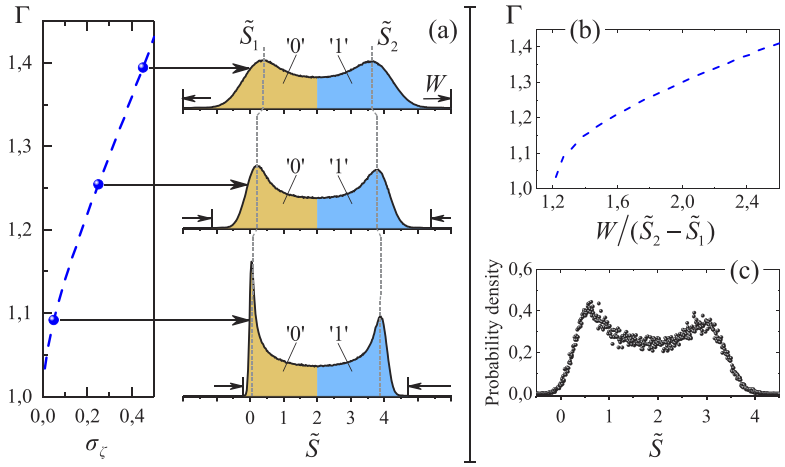


Fig. 3. (a) The theoretical dependence of the quantum reduction factor Γ on the photodetector noise width σ_ζ in case of digitization of the interference signal by the comparator. Monte-Carlo simulations of the PDF of the interference signal $\tilde{S}$ corresponding to the three different values of σ_ζ are shown to the right of the curve. (b) The theoretical dependence of the quantum reduction factor Γ on the PDF broadening factor $B = W/(\tilde{S}_2 - \tilde{S}_1)$. (c) Experimental PDF of the interference signal.

To determine the signal PDF, we propose to sweep the comparator C0 threshold voltage, V_{th}^0, recording a random bit sequence of a specified length for each value of V_{th}^0 and calculating then the corresponding ratio of ones and zeroes in the current sequence: $R = N_{ones}/N_{zeroes}$. One can then restore the value of the signal PDF corresponding to the i-th value of V_{th}^0 using the following relation:

$$f_{\tilde{S}}^i = \frac{|R_i - R_{i+1}|}{\Delta V(1 + R_i + R_{i+1} + R_i R_{i+1})}, \tag{16}$$

where ΔV is the voltage sweep step. Note that throughout the article by photodetector or comparator voltage we mean dimensionless quantity related to the normalized signal $\tilde{S}$ and not to the signal in volts.

Generally, only a single comparator, C1 or C2, is needed to obtain a random output, so let us assume for now that only one of them is used. The purpose of the second comparator will be clarified shortly. By definition, if the photodetector signal exceeds the threshold voltage of the comparator, the latter outputs a logical one, otherwise the signal from the comparator corresponds to a logical zero. The threshold voltage should be chosen so that the ratio of the number of ones to the number of zeros in the output random sequence was close to unity. Since we know the signal PDF $f_{\tilde{S}}$ found with the comparator C0, we can calculate the threshold voltage by defining it such that the areas under $f_{\tilde{S}}$ left and right of the threshold were equal.

Using an arrangement with a single working comparator, we acquired the 1Mbit random sequences. The data were then extracted from the FPGA buffer and stored as binary files on the PC. All of them successfully passed all NIST tests [30]. The result of the NIST statistical suite for one of the obtained sequences is shown in Fig. 4(b).

As mentioned above, the raw random bit sequences cannot be employed despite the successful randomness tests, since the raw signal is "diluted" by the classical noise. So, these sequences should be subject to randomness extraction procedure and thus the quantum reduction factor should be calculated. Unfortunately, the formulas for Γ given above cannot be applied directly, since the calculation of H_∞ with Eq. (11) requires the knowledge of $\tilde{S}_{min}$, which defines the

Optics EXPRESS

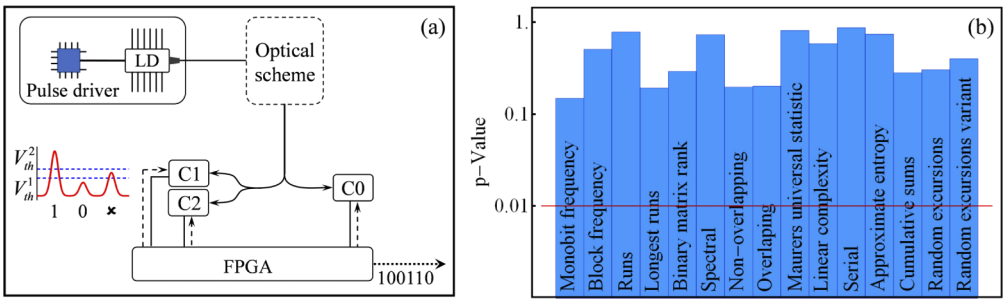


Fig. 4. (a) The schematic diagram of the QRNG: C0, C1, and C2 are high-speed comparators, LD is the laser diode, V_{th}^1 and V_{th}^2 in the inset stand for the threshold voltages of the comparators C1 and C2, respectively. (b) The result of the NIST statistical suite for one of the obtained raw random bit sequences. To pass the test we imposed the condition:p-Value ≥ 0.01.

integration limits. Obviously, one cannot calculate $\tilde{S}_{min}$ knowing only $f_{\tilde{S}}$; therefore, other approach should be used.

One of the possible methods is the substitution of $\tilde{S}_{min}$ by the value of the normalized integral signal $\tilde{S}_1$ corresponding to the left maximum of the PDF. In fact, one can see from Fig. 3(a) that $\tilde{S}_1$ is quite close to the left asymptote of $f_{\tilde{S}}^Q$ (i.e. to $\tilde{S}_{min}$), if the classical Gaussian noise is quite small. However, this maximum shifts to the right when increasing the classical noise contribution, which obviously overestimates the value of Γ. In fact, this method applied to the experimental PDF shown in Fig. 3(c) provides $\Gamma = 2.23$, which is unreasonably high.

Alternatively, one can use the fact that the PDF becomes broader when increasing the classical noise. For definiteness, we will assume that the width W of the distribution $f_{\tilde{S}}$ corresponds to the range, where $f_{\tilde{S}} > 10^{-5}$ (see Fig. 3(a)). Note that this choice is arbitrary, and with the same success one could take, e.g., $f_{\tilde{S}} > 10^{-4}$; however, this will obviously change abscissa values in Fig. 3(b). Therefore, it is important to choose the same assignation for both theoretical and experimental PDFs when calculating W. The "distance" between its maxima, in turn, decreases, so we can introduce the dimensionless quantity $B = W \big/ (\tilde{S}_2 - \tilde{S}_1)$, which reflects the contribution of classical noises. Here, $\tilde{S}_1$ and $\tilde{S}_2$ stand for the values of the integral signal, corresponding to the left and right maximum of $f_{\tilde{S}}$, respectively (see Fig. 3(a)). The dependence $\Gamma(\sigma_\zeta)$ can be thus substituted by the dependence $\Gamma(B)$, which is shown in Fig. 3(b). The main advantage of this representation is that B does not depend explicitly on H_∞ and can be easily calculated from the experimental PDF. The value of Γ can be then easily found from Fig. 3(b). We estimated the experimental value of the broadening factor to be $B = 1.77$, which provides $\Gamma = 1.25$. Comparing the PDF shown in Fig. 3(a) in the middle (it corresponds to $\Gamma \approx 1.25$) with the experimental one shown in Fig. 3(c), it becomes obvious that this estimate is more reasonable. So, after the RE procedure (we used hashing) the raw random sequence is reduced by a factor 1.25 resulting in the random bit generation rate of 2 Gbps.

Finally, let us consider the role of the comparators C1 and C2 and show how the quantum noise can be extracted without post-processing. Note that if the photodetector signal falls near the center of the PDF, i.e. if the photodetector output is close to the comparator threshold, then there is a high probability that the resulting bit is forged by an intruder. In fact, in this case an adversary could "toss" the output left and right of the threshold using his influence on the classical noise. Therefore, one should discard signals corresponding to some region near V_{th} in order to avoid intrusion of an adversary. The width of such a region should be guaranteed to be larger than the width of classical fluctuations. Discarding untrusted bits is analogous to the reduction of the output sequence, so the width of the "untrusted region" should be related to the value of the quantum reduction factor Γ. Denoting the area under $f_{\tilde{S}}$ between the boundaries of the untrusted

Optics EXPRESS

region as P and taking into account that the remaining area is $1 - P$, we can define the quantum reduction factor as follows: $\Gamma = 1/(1 - P)$. The value of P, in turn, can be defined by the integral

$$P = \int_{V_{th}-\Delta V_\Gamma^1}^{V_{th}+\Delta V_\Gamma^2} f_{\tilde{S}}(x)dx, \tag{17}$$

where ΔV_Γ^1 and ΔV_Γ^2 are "untrusted intervals" left and right of the threshold. One can see from Fig. 3 that the PDF is quite symmetric in the vicinity of V_{th}, so one can put $\Delta V_\Gamma^1 = \Delta V_\Gamma^2 = \Delta V_\Gamma$ and using the definition of Γ in terms of P write the following relation:

$$\int_{V_{th}}^{V_{th}+\Delta V_\Gamma} f_{\tilde{S}}(x)dx = \frac{\Gamma - 1}{2\Gamma}, \tag{18}$$

which defines the interval ΔV_Γ.

Afterall, the threshold voltages of the comparators C1 and C2 are set to $V_{th}^1 = V_{th} - \Delta V_\Gamma$ and $V_{th}^2 = V_{th} + \Delta V_\Gamma$, respectively. The digital output from the two comparators should be then added modulo 2. Let us denote the output of the comparators C1 and C2 as c_1 and c_2, respectively. If $c_1 \oplus c_2 = 0$, then the FPGA buffers c_1 or c_2 (either one of them, since they are the same in this case). If, however, $c_1 \oplus c_2 = 1$, then nothing is written to the buffer (see the inset in Fig. 3(a)). So, discarding the signal that falls into the range from $V_{th} - \Delta V_\Gamma$ to $V_{th} + \Delta V_\Gamma$, we improve the reliability of the random bit sequence. This method can be thus considered as a hardware quantum randomness extractor.

Let us summarize the working process of the QRNG presented in Fig. 4(a). We assume first that the laser continuously generates short pulses at 2.5GHz repetition rate. The working cycle of the QRNG starts with the calculation of $f_{\tilde{S}}$ with the comparator C0 using Eq. (16). For this, one should specify the step ΔV of the threshold voltage sweep and the number of bits that will be used to find ratio of ones and zeroes at each value of V_{th}^0. Calculated density distribution is then saved as an array in the memory. Then the threshold V_{th} is calculated such that the areas under $f_{\tilde{S}}$ left and right of V_{th} were equal. Then the PDF broadening factor B is calculated and the quantum reduction factor Γ is determined from the theoretical dependence $\Gamma(B)$. Knowing Γ and V_{th} the system calculates ΔV_Γ with Eq. (18) and sets threshold voltages for the comparators C1 and C2. In parallel, the system again starts calculating $f_{\tilde{S}}$, V_{th} and Γ performing thus the on-the-fly control of the QRNG operation. Afterwards, the FPGA starts buffering random bits checking for each sample the result of the XOR operation of the digital signals from the comparators and discarding the samples for which $c_1 \oplus c_2 = 1$.

Note that the embodiment of the QRNG with a single working comparator, where the post-processing is employed, is somewhat equivalent to the implementation with the two comparators C1 and C2, where the hardware quantum randomness extraction is performed. However, due to its simplicity, the latter seems to us more preferable. Note also that the raw random bit sequences were already "random enough" to pass the statistical tests, so processed sequences obviously pass them too; therefore, we do not present the results of the tests here.

It is important to mention that despite the ideological similarity between the post-processing procedure and the hardware quantum randomness extraction presented here, they do different jobs. Conventional randomness extractors assume that the pseudorandom sequence is somehow correlated, and these correlations are removed with the use of, e.g., cryptographic hash-functions, which transform the raw sequence such that it becomes unrecognizable. The quantum randomness extraction procedure developed here assumes that quantum noise is truly random by default, but the whole noise of the system is contaminated by classical noise, which could be (albeit not necessarily) correlated. In contrast to hashing, the proposed hardware quantum noise "extractor"

Optics EXPRESS

does not remove correlations from the bit sequence but eliminates the contribution of classical noise. Acquired random bit sequence is then assumed to be related to the pure quantum noise and thus considered to be perfectly random. If we compare the raw sequence and the sequence obtained after our extractor, they will be very similar, with the only difference being that some bits in the "pure quantum" sequence will be skipped. Therefore, it is not quite correct to compare the hardware "extractor" reported here with conventional randomness extractors developed for pseudo-random numbers in terms of latency, usability or speed. The only common feature between them is the measure of reduction of the raw sequence length, which is defined by the quantum reduction factor Γ. Note also, that the proposed hardware quantum noise extractor was defined only for the scheme with the comparator. For the scheme with an ADC, the method described above is not applicable, since one cannot just "cut off" the center of the signal PDF in this case.

6. Conclusions

We demonstrated a simple method of quantum noise extraction from the interference of laser pulses. The developed approach is based on the calculation of the quantum reduction factor Γ, which allows determining the contributions of quantum and classical noises in the assumption that classical fluctuations exhibit Gaussian PDF. To the best of our knowledge, the concept of the quantum reduction factor is introduced for the first time. It was shown how to calculate Γ for the case, when an ADC is used to digitize the signal, as well as for the case when the comparator is used for the digitization.

A robust scheme of the QRNG with the random bit generation rate of 2 Gbps was proposed. We developed a method for the on-the-fly control of the QRNG operation based on the continuous calculation of the signal PDF followed by the hardware randomness extraction. Due to its simplicity, the proposed randomness extraction procedure seems to be a good alternative to conventional post-processing procedures employing cryptographic hash-functions, Toeplitz extractors, etc.

Appendix

As we mentioned in the main text, semiconductor laser phase fluctuations are well described by the Langevin equations in terms of phase diffusion [11]. The random phases of laser pulses φ_p can be assumed to be distributed according to the normal law with an rms of σ_φ, whereas the phase difference $\Delta\varphi_p$ between the two different laser pulses also has a normal PDF with an rms to be $\sigma_{\Delta\Phi} = \sigma_\varphi\sqrt{2}$. The PDF of the phase difference $\Delta\Phi = \Delta\varphi_p + \Delta\theta$ may be then written in the following form

$$f_{\Delta\Phi}(x) = \frac{1}{\sigma_{\Delta\Phi}\sqrt{2\pi}} \exp\left(-\frac{(x-\Delta\theta)^2}{2\sigma_{\Delta\Phi}^2}\right). \tag{19}$$

Since $\Delta\Phi$ is in the argument of the cosine (Eq. (1) in the main text), then taking into account that the value of $\cos(\Delta\Phi)$ will not change neither after the substitution $\Delta\Phi \to \Delta\Phi + 2\pi j$ (j is integer) nor after the change of the sign $\Delta\Phi \to -\Delta\Phi$, we can write $f_{\Delta\Phi}$ as follows:

$$f_{\Delta\Phi}(x) \leftrightarrow \begin{cases} \sum\limits_{p=\pm1}\sum\limits_{j=-\infty}^{\infty} f_{\Delta\Phi}(px+2\pi j),\ x \in [0,\pi) \\ 0,\quad x \notin [0,\pi) \end{cases}, \tag{20}$$

whence

$$f_{\Delta\Phi}(x) = \frac{J\left(\frac{x}{2} - \frac{\Delta\theta}{2}, e^{-\sigma_{\Delta\varphi}^2/2}\right) + J\left(\frac{x}{2} + \frac{\Delta\theta}{2}, e^{-\sigma_{\Delta\varphi}^2/2}\right)}{2\pi}, \tag{21}$$

Optics EXPRESS

where $J(u, q)$ is the Jacobi theta function:

$$J(u, q) = 1 + 2\sum_{j=1}^{\infty} q^{j^2} \cos(2ju). \tag{22}$$

Since in our case $q < 1$, the series in (22) rapidly converges, so the value of the theta function can be estimated with the use of just the two first terms:

$$J(u, q) = 1 + 2q \cos 2u. \tag{23}$$

It is obvious from Eq. (23) that the deviation of $J(u, q)$ from unity is determined by the factor $2q = 2\exp(-\sigma^2_{\Delta\Phi}/2)$. Already at $\sigma^2_{\Delta\Phi} = (2\pi)^2$ we have $2q \sim 10^{-8}$, so one can assume with great accuracy that

$$f_{\Delta\Phi} = \begin{cases} \frac{1}{\pi}, & \Delta\Phi \in [0, \pi) \\ 0, & \Delta\Phi \notin [0, \pi) \end{cases}, \tag{24}$$

if $\sigma_{\Delta\Phi} = \sigma_\varphi\sqrt{2} > 2\pi$.

Funding

Russian Science Foundation (17-71-20146).

Disclosures

The authors declare no conflicts of interest

References

1. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**(1), 015004 (2017).
2. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**(10), 711–715 (2010).
3. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," Opt. Express **19**(21), 20665–20672 (2011).
4. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express **22**(2), 1645–1654 (2014).
5. Q. Zhou, R. Valivarthi, C. John, and W. Tittel, "Practical quantum random-number generation based on sampling vacuum fluctuations," Quantum Eng. **1**(1), e8 (2019).
6. Y. Mansour, N. Nisan, and P. Tiwari, "The computational complexity of universal hashing," Theor. Comput. Sci. **107**(1), 121–133 (1993).
7. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A **87**(6), 062327 (2013).
8. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**(11), 12366–12377 (2012).
9. F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, and J. C. F. Matthews, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Opt. Express **26**(16), 19730–19741 (2018).
10. C. Henry, "Theory of the linewidth of semiconductor lasers," IEEE J. Quantum Electron. **18**(2), 259–264 (1982).
11. C. Henry, "Phase noise in semiconductor lasers," J. Lightwave Technol. **4**(3), 298–311 (1986).
12. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104**(26), 261112 (2014).
13. C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, "Generation of Fresh and Pure Random Numbers for Loophole-Free Bell Tests," Phys. Rev. Lett. **115**(25), 250403 (2015).
14. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," Phys. Rev. Lett. **98**(23), 230501 (2007).
15. D. E. Knuth, *The Art of Computer Programming* (Addison-Wesley, 1997).
16. A. Aspect, "Bell's inequality test: more ideal than ever," Nature **398**(6724), 189–190 (1999).

Optics EXPRESS

17. N. Nisan and A. Ta-Shma, "Extracting Randomness: A Survey and New Constructions," J. Comput. Syst. Sci. **58**(1), 148–173 (1999).
18. L. Trevisan, "Extractors and pseudorandom generators," J. Assoc. Comput. Mach. **48**(4), 860–879 (2001).
19. K. Petermann, *Laser Diode Modulation and Noise* (Kluwer Academic Publishers, 1988).
20. O. Svelto, *Principles of Lasers* (Springer, 2010).
21. R. Loudon, *The Quantum Theory of Light* (Oxford University, 2000).
22. R. J. Glauber, "Nobel Lecture: One Hundred Years of Light Quanta," Rev. Mod. Phys. **78**(4), 1267–1278 (2006).
23. A. N. Oraevskii, "Spontaneous emission in a cavity," Phys.-Usp. **37**(4), 393–405 (1994).
24. I. R. Senitzky, "Phase correlation in cascade spontaneous emission by a multilevel system: atomic memory," J. Opt. Soc. Am. B **1**(6), 879–881 (1984).
25. R. H. Dicke, "Coherence in Spontaneous Radiation Processes," Phys. Rev. **93**(1), 99–110 (1954).
26. K. Nakata, A. Tomita, M. Fujiwara, K.-I. Yoshino, A. Tajima, A. Okamoto, and K. Ogawa, "Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution systems," Opt. Express **25**(2), 622–634 (2017).
27. V. S. Pugachev, *Probability Theory and Mathematical Statistics for Engineers* (Oxford University, 1984).
28. L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," Opt. Express **24**(16), 17849–17859 (2016).
29. R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinsky, V. Kurochkin, and Y. Kurochkin, "Influence of chirp, jitter and relaxation oscillations on laser pulse interference in optical quantum random number generator," to be published
30. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22 revision 1a (2010).