A tunable quantum random number generator based on a fiber-optical Sagnac interferometer

To cite this article: Joakim Argillander et al 2022 J. Opt. 24 064010

You may also like

- Semi-device independent randomness generation based on quantum state's indistinguishability
  Hamid Tebyanian, Mujtaba Zahidy, Marco Avesani et al.

- Estimating the privacy of quantum-random numbers
  Johannes Seiler, Thomas Strohm and Wolfgang P Schleich

- Enhanced security for multi-detector quantum random number generators
  Davide G Marangoni, Giuseppe Vallone, Ugo Zanforlin et al.
A tunable quantum random number generator based on a fiber-optical Sagnac interferometer

Joakim Argillander*©, Alvaro Alarcón© and Guilherme B Xavier©

Institutionen för Systemteknik, Linköping University, 581 83 Linköping, Sweden
E-mail: joakim.argillander@liu.se
Received 20 January 2022, revised 4 April 2022
Accepted for publication 21 April 2022
Published 6 May 2022

Abstract
Quantum random number generators (QRNGs) are based on naturally random measurement results performed on individual quantum systems. Here, we demonstrate a branching-path photonic QRNG implemented using a Sagnac interferometer with a tunable splitting ratio. The fine-tuning of the splitting ratio allows us to maximize the entropy of the generated sequence of random numbers and effectively compensate for tolerances in the components. By producing single-photons from attenuated telecom laser pulses, and employing commercially-available components we are able to generate a sequence of more than 2 gigabytes of random numbers with an average entropy of 7.99 bits/byte directly from the raw measured data. Furthermore, our sequence passes randomness tests from both the NIST and Dieharder statistical test suites, thus certifying its randomness. Our scheme shows an alternative design of QRNGs based on the dynamic adjustment of the uniformity of the produced random sequence, which is relevant for the construction of modern generators that rely on independent real-time testing of its performance.

Keywords: quantum random number generation, tunable beamsplitter, fiber-optic Sagnac interferometer

(Some figures may appear in colour only in the online journal)

1. Introduction
Quantum information science is an interdisciplinary field where computer science meets physics, and where long lasting principles of information transfer, cryptography and secret sharing are challenged [1]. Quantum random number generators (QRNGs) are mature devices that directly benefit from the properties of quantum systems in order to produce truly random numbers [2]. By harnessing the fundamental randomness from the outputs of quantum mechanical measurements it is possible to generate sequences of fundamentally unpredictable random numbers. A popular implementation for QRNGs is based on performing measurements on single-photons. Typically, in these photonic QRNGs, one degree of freedom of a photon is used to prepare a superposition state of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$, which is then projected onto the basis formed by $|0\rangle$ and $|1\rangle$. By letting one of the basis vectors represent a binary ‘0’ and the other a binary ‘1’, we can utilize the fact that measurements of an equally weighted superposition state yield uniformly distributed random measurement outcomes to generate a random sequence by performing repeated measurements.

One type of photonic QRNG is known as a branching-path generator [2–6], and is typically implemented either using polarized light and polarizing beamsplitters, or with

* Author to whom any correspondence should be addressed.

Original Content from this work may be used under the terms of the Creative Commons Attribution 4.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
unpolarized light and conventional beamsplitters. Regardless of the scheme, it is of utmost importance that the beamsplitters’ splitting ratio is 50:50 for transmitted and reflected light respectively, in order to guarantee an unbiased sequence. In practice, due to manufacturing limitations, the splitting ratio will not be perfectly balanced, and this leads to non-uniformity of the bit distribution of the generated sequence. Furthermore, the splitting ratio may also change over time, due to temperature fluctuations and other environmental factors, as well as component degradation. Branching-path generators may also suffer from detector imbalances, where two identical tunable devices used at each of the beamsplitter’s outputs have slightly different detection efficiencies that also lead to a bias in the sequence [2]. Such a bias reduces the unpredictability of the sequence, and also so does its usability, not only for cryptography, but also for uses like Monte-Carlo simulations and gambling. For cryptography specifically, the security is directly proportional to the randomness of the secret key, and therefore a low-entropy sequence increases the probability that an attacker is able to successfully guess the key, which thus reduces the effective strength of the cipher [7].

In this article, we demonstrate a tunable-ratio branching-path photonic QRNG by implementing a dynamically tunable beamsplitter using a fiber-optical Sagnac interferometer. The tunable beamsplitting function is implemented with an active phase modulator placed in a Sagnac loop working as a single-photon router [8]. By modulating the phase of a light packet propagating in the clockwise direction vs the counterclockwise one, we are able to tune the output probabilities from the Sagnac interferometer through a change in the amplitude of the driving signal fed to the phase modulator. This allows us to change the entropy of the generated sequence as we wish. Both outputs are then detected through a time-division multiplexing scheme to allow detection with only one single-photon detector. Interferometers in a Sagnac-type configuration have previously been used to modulate polarization [9, 10] and intensity [11] in order to prepare states for quantum key distribution experiments. While building on the same principle, our system is the first demonstration of interferometric routing of single photons for quantum random number generation. In this work we are able to generate a continuous stream of random numbers over 36 h of continuous operation at an average rate of 131 kbit s$^{-1}$. The generation rate and entropy are highly stable over time due to the intrinsic phase stability of the Sagnac interferometer configuration. We finally demonstrate the randomness of the sequence by passing it successfully through the stringent statistical test suites NIST 800–22 [12] and Dieharder [13] aimed at assessing random number generators. A critical issue in QRNGs, especially the ones aimed at cryptographic applications, is whether the user can trust the device. A solution to this problem is performing independent real-time testing of the internal devices of the QRNG, usually through the user changing either the prepared quantum states, or a measurement parameter [14]. In order to test the device and achieve high confidence that the generated sequence is private, a high interferometric visibility is necessary [15]. The dynamic tunability provided by our setup is therefore useful to tackle this issue, and is particularly appealing to recently demonstrated measurement-device-independent QRNGs [15, 16]. Our results show that Sagnac interferometers can be successfully employed as tunable beamsplitters for the construction of QRNGs, thus opening up for implementation of state-of-the-art measurement-device independent QRNGs.

2. The experiment

The principle for a QRNG scheme using a TBS is based on a source of strongly attenuated pulses, a beamsplitter with a variable splitting ratio and single-photon detection of the two outputs of the beamsplitter (figure 1). A detection at one output is assigned the bit ‘0’, while ‘1’ is assigned to the other one. The entire system works synchronously, driven by field programmable gate array (FPGA) electronics, which also performs the data acquisition. If both outputs are simultaneously detected (either from two photons generated together, or from noise sources), the FPGA discards that result in order to remove the effects of after-pulsing and multiphoton events. Similarly, if no photons are detected for a generated pulse (due to absorption) no result is recorded. The generated bits are then streamed from the FPGA to a personal computer for randomness extraction and storage. The bitstream then passes through statistical tests to certify its randomness.

The key aspect in our experiment is the use of a tunable beamsplitter (figure 1). Although in principle it is possible to create one by adding extra attenuators in each output of a conventional beamsplitter, or by using a half-wave plate in tandem with a polarizing beamsplitter, these options do not provide possibilities of fast tuning. Furthermore, in the case of the first option, extra losses are added to the system. Here we pursue an interferometric approach to implement tunability. For instance, a Mach-Zehnder interferometer can realize a tunable beamsplitter, with the tunability provided by setting the relative phase $\phi$ between the interferometer arms [17]. The output probability of the single-photon is then given by a sinusoidal function of $\phi$. However, the drawback of using conventional Mach-Zehnder interferometers is that they suffer from intrinsic phase instability, and therefore require either mechanical isolation (i.e. dampened tables, environmental protection, etc) [18] or active stabilization [19, 20]. In our work we follow the approach of [8] where we employ a Sagnac interferometer to provide the same functionality, with the added benefit of intrinsic phase stability. In our Sagnac interferometer a high-speed telecom fiber-pigtalled phase modulator is placed to give a relative phase shift $\phi$ between the two propagation directions (figure 2). This is done by synchronizing the phase shift with the wave packet, such the phase shift is only applied in one direction by the modulator.

We employ a continuous wave (CW) distributed feedback telecom laser diode, centered at $\lambda = 1546.92$ nm, connected to variable optical attenuators (ATT) to produce weak coherent states. The FPGA board generates electrical pulses at a repetition rate of 250 kHz in order to drive an intensity modulator.
which chops the CW input light into optical pulses. The electronic pulses are shaped to 20 ns width, as limited by the employed electronics driver before being fed to the intensity modulator. The attenuated optical pulses pass through an optical circulator before entering one of the input ports of a bidirectional 50:50 fiber coupler. The output ports form the Sagnac loop, together with a phase modulator and a 50 m long optical fiber spool (Ls) that works as a delay line (figure 2). The delay line is needed to ensure there is sufficient time separation for the phase modulation signal to act on the wave packet propagating in only one direction and not in the opposing one, thus creating the necessary relative phase shift to generate the different output probabilities in the interferometer outputs [8]. Not shown in figure 2 are two manual polarization controllers added in the Sagnac loop, where one is used to align the pulses’ polarization with the input polarization of the phase modulator, while the second one is used to ensure that the two counter-propagating terms have the same polarization at the recombining beamsplitter.

Inside the Sagnac loop the attenuated pulses can be represented as a coherent superposition of the two counter-propagating paths as

$$|\psi\rangle = \sqrt{3}/2|\text{CW}\rangle + i e^{i\phi}|\text{CCW}\rangle$$

where |CW⟩ and |CCW⟩ represent the clockwise and counterclockwise propagation paths respectively. The detection probabilities at the outputs A and B of the Sagnac loop are proportional to \(\cos^2(\frac{\phi}{2})\) and \(\sin^2(\frac{\phi}{2})\). For voltages corresponding to \(\phi = \pi/2, 3\pi/2\) the Sagnac works as a beamsplitter with a perfectly balanced splitting ratio. The phase shift \(\phi\) is proportional to the modulator’s driving voltage, thus allowing us to precisely control the splitting ratio between 0 and 1 in the ideal case. We fine-tune the desired ratio by applying a small offset \(\delta V_\phi\) to the theoretical voltage value \(V_\phi\). Therefore, the voltage we apply to achieve a balanced splitting ratio is

$$V_{\pi/2} = V_{\pi/2} + \delta V_{\pi/2}.$$  

Due to insertion losses and propagation losses in the time-bin multiplexer, a balanced splitting ratio between the early and late time bin does not imply a 50:50 probability for a photon to emerge at the outputs A:B of the Sagnac interferometer. The two outputs of the Sagnac (denoted A and B in figure 2) are then routed to the detection system (with output A passing through the circulator to decouple it from the attenuated pulses coming from the source, propagating in to the Sagnac loop). We opted to use one SPD and mapped each output path to an early or a late time-bin, with both time slots detected sequentially by the SPD. The time-bin separation is created by a 750 ns time delay (\(\approx 150\ m\) optical fiber spool) placed at the A output path from the Sagnac loop. The two paths are then recombined with a 50:50 bidirectional fiber coupler, and one of its outputs is connected to the SPD (idQuantique id210), operating in Geiger mode with 10% detection efficiency, 2.5 ns gate width and approximately 10⁻⁵ dark count probability per gate. The SPD is externally gated by the FPGA by sending pairs of pulses, each separated by the time-bin delay, that are synchronized with the signal sent to the intensity modulator that generates the photon pulses. Each of these pulses correspond to a gate in the early and late bin respectively. The output signals from the SPD are also read by the FPGA for data acquisition. We set the deadtime of the SPD to 500 ns, so that it is shorter than the time separation between the early and late time-bins. We then let a detection of a photon in the early time-bin represent a ‘0’ and a detection in the late time-bin represent a ‘1’.

### 3. Results

First we demonstrate the variable splitting ratio of the Sagnac interferometer acting as a tunable beamsplitter. We set the attenuators such that we maximize the detection probability at the detector for both time-bins, while still operating in a linear regime (i.e. the detector is not saturating). This is observed from figure 3(a), where the number of detection events per integration time fits well with the theoretical prediction that output A [B] from the Sagnac loop should follow a \(\cos^2(\frac{\phi}{2})\) \([\sin^2(\frac{\phi}{2})]\) distribution. We also observe from these results that the Sagnac interferometer is operating correctly, and complementary output behavior of the two outputs is observed, as expected.

We then wish to optimize the operating point of the Sagnac loop for optimal random number generation. We scan the driving voltage of the phase modulator and measure the Shannon entropy of the generated bits when considered as 8-bit symbols. The Shannon entropy \(H\) is defined as

$$H = -\sum_{i=0}^{255} p_i \log_2(p_i),$$

where \(p_i\) is the probability of finding the \(i_{th}\) 8-bit sequence. We increase the voltage \(V_\phi\) applied to the phase modulator in the range 0 \(\leq V_\phi \leq 4.2\) in steps of 200 mV and measure the entropy, as can be seen in figure 3(b). An inset is shown in figure 3(b) where we also sweep the voltage between 2 and 2.3 V in steps of 20 mV, and likewise measure \(H\) to identify the optimal operating point where the entropy is maximized. It can be clearly seen that the maximum obtained entropy (7.98 bits/byte) occurs for an applied driving voltage of around 2.15 V.

With the entropy maximized, we then proceed to acquire a long continuous sequence of bits to feed to the statistical randomness tests, and also to demonstrate the robustness of our implementation. The raw bit sequence is buffered in the FPGA in blocks of 32 kilobytes and then transmitted over an Ethernet connection to a personal computer for storage. Before

---

**Figure 1.** Principle of a tunable-ratio beamsplitter for quantum random number generation. Light from a photon source is split using a tunable beamsplitter (TBS). Detectors (D1, D2) placed at the outputs of the TBS register photon events and record a binary ‘0’ or a binary ‘1’ depending on whether the photon impinges on D1 or D2. The choice of assignment of ‘0’/‘1’ to D1/D2 is arbitrary.
Figure 2. Experimental setup. The CW-laser is first fed to an intensity modulator (IM) that chops the laser into 20 ns pulses, which are then attenuated using a variable attenuator (ATT) to weak coherent pulses (WCPs) with an average photon probability of approximately ten photons per pulse. The WCPs are then fed to a Sagnac interferometer that acts as a tunable beamsplitter where the superposition $|\psi\rangle = \frac{1}{\sqrt{2}} (|CW\rangle + i e^{i\phi} |CCW\rangle)$ is prepared, and CW and CCW denote the photon state of propagation inside the Sagnac loop. At the output of the Sagnac loop, we use a 150 m fiber-optic delay line ($L_{TB}$) to add $\approx 750$ ns of delay to one term, effectively time-bin multiplexing the two outputs from the Sagnac interferometer into an early and a late time-bin for detection using one single-photon detector.

Figure 3. (a) Characterization of detected photon events measured in the early and late time-bin, as a function of applied voltage to the phase modulator. The error bars are calculated assuming Poissonian photon statistics ($\sigma = \sqrt{N}$ for a photon count of $N$). Also plotted is a fit of the theoretical detection probabilities that are proportional to $\cos^2[\sin^2]$ for the early [late] time-bin, respectively. (b) Raw entropy (before extraction) as a function of applied voltage to the phase modulator. Also shown in the inset is a plot of the entropy versus applied voltage to the phase modulator with a smaller step size.

assessing the sequence, it is passed through a Toeplitz randomness extraction procedure in order to remove any remaining non-uniformities from the raw data. To extract randomness, we split the generated sequence into $N$ sequences of length $n$, and multiply each subsequence with an $n \times m$ binary Toeplitz matrix which yields an output of $m$ hashed bits [21]. We choose to use $n = 400$, and as defined in [21], we obtain $m = H_{\text{min}} = 2 \log_2 e$ where $H_{\text{min}}$ is the min-entropy of 8-bit strings which is
defined as $H_{\min} = - \log_2 \left[ \max_{x \in \{0, 1\}} \Pr \{X = x\} \right]$. We measure a min-entropy of 7.7451 from the acquired sequence before extraction. We choose a security parameter $\varepsilon = 2^{-100}$ which is derived from the leftover hash lemma [22]. We seed the Toeplitz matrix $T$ at the beginning of the extraction procedure with $n + m - 1$ bits taken from the raw sequence, as it is sufficient to only specify the first row and first column. The matrix $T$ can be reused for each of the subsequences, and we obtain the extracted sequence of bits by concatenating the results of the multiplications $T_{n1}, T_{n2}, T_{n3}, \ldots, T_N$, where the subscript represents the subsequence index [21, 22]. The extraction procedure is lossy, and for our choice of parameters, we are able to achieve an efficiency of $\approx 50\%$. After extraction we calculate the min-entropy of the sequence to be $7.9982$ bits.

While recording the raw data, we also measure the entropy of each streamed 32 kilobyte block, and as can be seen in figure 4(a), we achieve an average entropy of $\approx 8.0014$ bits/byte over $36$ h, which demonstrates exceptional phase stability of the QRNG. Likewise, we also measure the raw bitrate when streaming the data, and we achieve an average bitrate of $131.8 \pm 2.3$ kbps (figure 4(b)).

The bitrate is mainly limited by the delays in the electronics that amplify the signals from the FPGA in order to drive the phase modulator, and in the triggering electronics which is necessary to synchronize the generation of pulses with the detection. By improving the driver electronics, the bitrate is only limited by the separation of the time bins.

After generating $2.2$ gigabytes of data, and extracting it, we pass the sequence through the NIST 800-22 Statistical Test Suite [12] (NIST test) and the Dieharder [13] test suite. Both test suites subject the random sequence to a number of statistical tests aimed at assessing the randomness of any given sequence. We run the NIST tests with $1000$ bitstreams of length $1$ Mb. To deem any given test as passed, we form a confidence bound as defined in [12] for the proportion of bitstreams that must yield a $p$-value $p \geq 10^{-2}$ using the formula $\hat{p} \pm 3 \sqrt{\frac{\alpha(1-\alpha)}{n}}$ where $\alpha = 10^{-2}$, $n = 1000$ is the number of bitstreams and $\hat{p} = 1 - \alpha$. This gives us a confidence interval of $0.980 < r < 0.999$, and if the ratio of tests that have passed falls outside this range, there is evidence that the sequence is not random [12]. Figure 5 shows the proportions of tests that pass, for any given test category, along with the significance level.
Figure 6. Achieved visibilities for the states $|\Psi\rangle$ and $|\Phi\rangle$ that are expected to yield deterministic measurement results, together with the visibilities for the balanced state $|\Omega\rangle$ used for randomness generation.

The Dieharder test suite yields a verdict ('Fail', 'Weak', 'Pass') for each test, and a test is deemed to pass if the $p$-value associated with it is in the interval $10^{-2} < p < 1 - 10^{-2}$. As can be seen in figure 5(a), there are parameterized tests where each test yields multiple $p$-values (one for each value of the parameter). We plot all outputted $p$-values, and compute a resulting $p$-value from a Kolmogorov-Smirnov test of all the $p$-values. As is well-known, the $p$-values should be uniformly distributed under the null hypothesis that the sequence is indeed random, and the Kolmogorov-Smirnov test is used to eliminate false rejection of the null hypothesis (Type-I error) [23]. For three of the tests, we observe that the resulting $p$-values fall outside the confidence bound, and for those values of the parameter, the test verdict is 'weak'. Since the Dieharder suite is a statistical test, it is probable that there will be occasional 'weak' results. If the generator truly is weak, then it will certainly fail other tests [13].

To further demonstrate that the tunability can be used as a building block in measurement-device independent protocols we run a prepare-and-measure type protocol where we use the TBS to prepare either of the orthogonal states $|\Psi\rangle$ and $|\Phi\rangle$ which are expected to yield deterministic measurement results, and a state $|\Omega\rangle$ which yields random (but balanced) measurement outcomes. We prepare the states by applying different voltages to the PM inside the Sagnac for each state. From figure 3(a) we determine the voltages to be $V_\Phi = 0$ V, $V_\Psi = 4.2$ V and $V_\Omega = 2.15$ V. For each acquired 32 kilobyte block of data we then randomly choose between preparing either of the states with a probability $Pr\{|\Psi\rangle\} = Pr\{|\Phi\rangle\} = 0.005$ and $Pr\{|\Omega\rangle\} = 0.99$, where $Pr\{|\bullet\rangle\}$ is the probability to prepare a certain quantum state, in order to demonstrate the switching of states necessary to implement measurement-device independent QRNG protocols. In figure 6 we show the recorded visibilities for each of the states as a function of time, where the visibility $\nu_x \in [0, 1]$ for the state $x \in \{|\Psi\rangle, |\Phi\rangle, |\Omega\rangle\}$ is defined $\nu_x = \frac{n_{\text{early}} - n_{\text{late}}}{n_{\text{early}} + n_{\text{late}}}$ where $n_{\text{early}}$ and $n_{\text{late}}$ are the detector counts in the early and late bin respectively. We are able to achieve a mean visibility of $\nu_\Psi = 0.997 \pm 3.3 \times 10^{-2}$, $\nu_\Phi = 0.990 \pm 3.1 \times 10^{-3}$ and $\nu_\Omega = 0.004 \times 10^{-2} \pm 7.7 \times 10^{-3}$ for each of the three states without subtracting dark counts.

4. Conclusions

We have proposed and experimentally demonstrated a photonic QRNG based on a dynamically tunable beamsplitter. The random numbers are generated depending on which output from the beamsplitter the single-photons are detected. By tuning the beamsplitting ratio we are able to maximize the generated entropy of the random sequence. This also helps maximize the entropy in spite of differences in losses following the two outputs. We implemented the tunable beamsplitter through a Sagnac interferometer, in which the tunability is given by a relative phase between the two counter-propagating paths, applied with an electro-optical telecom phase modulator. This technique allows ultra-fast tunability, due to the short response time of the phase modulator.

We are able to generate a continuous stream of random numbers over 36 h of continuous operation, showing an average raw generation rate of 131 kbit s$^{-1}$ and an average generated entropy of 7.9925 bits per byte in the raw sequence, thus demonstrating a stable source of entropy. As the bitrate is mainly limited by internal delays in the employed driving electronics, by improving the driver circuitry, a considerable bitrate gain can be achieved. By reducing these delays, we would also reduce the lower limits on the time-bin spacing and thus the repetition rate can be increased. Our setup is robust and built using only off-the-shelf telecom fiber components, thus also showing the practicability of our setup. Our results can aid in future designs of dynamically tunable QRNGs, and serve as a foundation for measurement-device quantum random number generation due to ease of changing the beamsplitting ratio, through the appropriate selection of the applied phase in the Sagnac loop.

Our system also demonstrates that the tunable beamsplitter enables realization of measurement-device independent QRNGs thanks to the high visibility when measuring orthogonal states, as well the fact that the visibilities show minimal degradation over time.

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Acknowledgments

We acknowledge financial support from CENIIT Linköping University, the Swedish Research Council (VR 2017-04470), QuantERA grant SECRET (VR 2019-00392), the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT).

Author contributions

J A and A A conceived the work together with G B X. J A developed the electronic control system, and A A developed the optical system. Data analysis was done by J A with
assistance from G B X. The work was coordinated by G B X. All authors contributed to the writing of the manuscript.

**Conflict of interest**

The authors declare no competing interests.

**ORCID iDs**

Joakim Argillander  
https://orcid.org/0000-0002-8734-2833

Alvaro Alarcón  
https://orcid.org/0000-0003-4295-7364

Guilherme B Xavier  
https://orcid.org/0000-0002-8234-424X

**References**


[14] Ma X, Yuan X, Cao Z, Qi B and Zhang Z 2016 Quantum random number generation npj Quantum Inf. 2 16021


[23] Hung H M J, O’Neill R T, Bauer P and Kohne K 1997 The behavior of the p-value when the alternative hypothesis is true *Biometrics* 53 11