Quantum Photonic TRNG with Dual Extractor

Mitchell A. Thornton[0000-0003-3559-9511] and Duncan L. MacFarlane

Southern Methodist University, Dallas TX 75275, USA
{mitch, dmacfarlane}@smu.edu
http://lyle.smu.edu/~mitch/qirg

Abstract. An enhanced true random number generator (TRNG) architecture based on a photonic entropy source is presented. Photonic TRNGs are known to produce photon sequences at randomly distributed time intervals as well as random superimposed quantum states. We describe a TRNG architecture that takes advantage of both of these sources of entropy with a dual-source extractor function. We show that the amount of harvested entropy exceeds that compared to implementations comprised of only one of these sources. We also describe an implementation of a beam splitter used within the architecture that is suitable for implementation in a photonic integrated circuit that has been simulated and fabricated.

Keywords: TRNG · QRNG · Extractor function · Photonic Integrated Circuit · Hadamard.

1 Introduction

The lack of high-quality random number sources in otherwise secure systems has been the cause of several well-documented security breaches [4][12][15]. Many devices require a continuous supply of random values to support the implementation of various modern cryptographic methods. It is desirable for the generation of random bit streams to be accomplished at high data rates to support applications such as modern secure high-speed communications. This need is coupled with the added constraint that random values must be of very high quality in terms of their independence and other statistical properties in order to preserve the integrity of encryption protocols. Additionally, high-speed and high-quality random number generators should be as inexpensive, rugged, and reliable as possible when the hosting devices are intended to be mass-produced.

The physical sources used in true random number generators (TRNG) are sometimes referred to as "weakly random sources" since it is practically impossible to measure or observe the source output without adding some degree of determinism, bias, or correlation. For this reason, TRNGs also incorporate extractor functions, or simply "extractors," that transform the output of a weakly random source into an equally likely and independent string of random bits. Many different weakly random sources have been identified and used in TRNGs, such as those based upon quantum effects, electronic metastability, electronic chaos generation, radioactivity, thermal effects, atmospheric effects, deep space radiators, and others. Because the theory of observing the results of quantum mechanical interactions is based on probabilistic axioms, entropy sources that rely upon the measurement or observation of superimposed quantum state information are considered here and have been used in the past [3]. We utilize such a source with photonic information carriers and show how two independent bit streams may be extracted in an efficient manner with only minor architectural changes required as compared to previous photonic architectures.

2 Quantum Photonic TRNG Architecture

In general, TRNGs are comprised of a physical source, an observation or measurement stage, and a post-measurement processing stage known as an "extractor" function, as shown in Fig. 1. The purpose of the extractor is to discard the undesired biases, correlations, and other deterministic components in the source measurements and to transform random values to output values that are as close as possible to being independent and equally likely. From an information theoretic point of view, the goal of the TRNG extractor is to maximize the information entropy in the output values by utilizing as much of the entropy present in the physical source as possible. Furthermore, the extractor function ideally produces values that are independent and uniformly distributed regardless of the native distribution of the physical source observations. For at least these reasons, extraction functions are very important with regard to the quality of TRNG output values. We propose a TRNG implemented in a Quantum Photonic Integrated Circuit (QPIC) using location-encoded (*aka*, "dual-rail") methods for information representation.

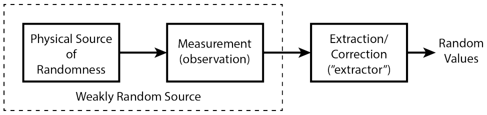
Physical Source of Randomness
Measurement (observation)
Weakly Random Source
Extraction/ Correction ("extractor")
Random Values

Fig. 1. A generic and typical TRNG block diagram including a physical source and extractor function.

We propose an architecture wherein a single photon pump excites a spontaneous parametric down conversion (SPDC) device to generate a heralded single photon source in the form of a signal and idler photon pair. The signal is then applied to a 50-50 beam splitter, used as a Hadamard operator, that drives the two waveguides representing orthogonal basis states, $|0\rangle$ and $|1\rangle$. The idler photon is transmitted in a third waveguide that enables a heralded implementation. Each of the three waveguides drives a single-photon avalanche diode (SPAD) detector that we denote as SPAD-0, SPAD-1, and SPAD-T. Thus, a random bit stream is produced depending upon which of SPAD-0 and SPAD-1 indicate energy detection that is correlated in time with an active output from SPAD-T. This approach for implementing a TRNG using photonic quantum effects is well-known and variations of this approach are used in commercial devices [2][10][11][14][16]. Fig. 2 contains a diagram illustrating this approach.

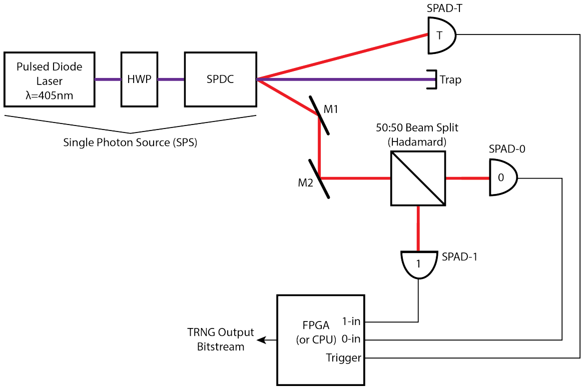

Fig. 2. A TRNG comprised of SPS, SPDC, and three SPADs.

As an example, the single photon source (SPS) in Fig. 2 is comprised of a pulsed laser source with wavelength 405nm serving as a pump and a rotatable half-wave plate (HWP) for adjusting the angle of linear polarization of the pump photon with the optical axis of the spontaneous parametric down converter (SPDC). The down-converted signal and idler photons are at 810nm wavelength. The topmost beam in Fig. 2 is indicative of the idler and is detected by SPAD-T whereas the bottommost beam produced by the SPDC is indicative of the 810nm signal photon beam and is path adjusted via mirrors M1 and M2 prior to entering the beam splitter. The beam splitter serves as a location-encoded Hadamard operator thus causing the position state of the signal photon to be equiprobable. The two outputs of the beam splitter and the idler photon are applied to detectors, SPAD-0, SPAD-1, and SPAD-T that supply input signals to an FPGA or CPU. When the FPGA or CPU receives a heralded input due to detection from SPAD-0 or SPAD-1, a randomly generated bit is produced based on which detector was activated.

In practice, a microcontroller (not shown) will provide the proper quenching of the SPAD and will maintain its operation in Geiger mode. The heralding, or triggering modality of the TRNG in Fig. 2 also provides the counts that allow coincidence statistics to ensure the system operated in the quantum regime, in spite of detection imperfections and possible laser drift.

Our proposed architecture is the same as that shown in Fig. 2 with the exception that the FPGA or CPU core is programmed to take advantage of two sources of entropy from the SPS. A physical photon entropy source such as that in Fig. 2 exhibits two different and statistically independent random characteristics. The first is a sequence of measurements based upon whether energy is detected at SPAD-0 or SPAD-1 as just described. The second is the sequence of time intervals between photon detection at either SPAD-0 or SPAD-1. It is irrelevant whether detection occurs at either SPAD-0 or SPAD-1 with respect to the sequence of time intervals separating photon generation. Thus, the time interval sequence is statistically independent with respect to the sequence of generated bits due to SPAD-0 and SPAD-1. Therefore, we consider the SPS as providing two independent entropy sources that are statistically independent.

Recent past results indicate that TRNGs based upon two sources can be superior as compared to a single source TRNG [5][6]. Our two-source approach utilizes two random variables (RV) where one is a Bernoulli distributed RV, X, and the other is a time series of sub-Poissonian distributed time intervals denoted as RV Y that originate as characteristics of the same single SPS. The extractor for the Bernoulli distributed RV X with variate x_i is denoted $Ext_2(X)$ and utilizes the outputs of two single-photon avalanche diodes (SPAD) shown as SPAD-0 and SPAD-1 in Fig. 2. We denote the RV V with variate v_i as the extracted value of variate x_i. The RV V has two possible outcomes and hence the event space is $\mathbb{F}_2 = \{0, 1\}$.

We also utilize an extractor function, $Ext_r(Y; r)$, for the sub-Poissoinian distributed RV Y that was recently introduced in [18] and referred to herein as "[TT:18]." RV W with variate w_i is extracted from RV Y via the use of $Ext_r(Y; r)$. The variates, y_i, of Y as utilized in our proposed TRNG architecture are of the form of a discretized set of time intervals, $\varDelta t_i$. The w_i values are radix-R values in the form of a bitstring of length r that have values $w_i \in \mathbb{F}_r = \{0, 1, \cdots, 2^r - 1\}$ where the number of different bitstrings is also $|\mathbb{F}_r| = R$ and where $R = 2^r > 2$. The extractor function $Ext_r(Y; r)$ receives input from SPAD-T in Fig. 2 and is implemented in the FPGA or CPU core that is also shown in Fig. 2.

Because X and Y are statistically independent and uncorrelated, the overall composite extractor of our TRNG is formed from $Ext_2(X)$ and $Ext_r(Y; r)$ and is denoted as $Ext(X, Y; r) = Ext_2(X)||Ext_r(Y; r)$ where $||$ denotes the concatenation operation. The order of concatenation is arbitrary and irrelevant. Generally, any arbitrary permutation of the bitstrings resulting from $Ext(X, Y; r)$ would suffice due to the fact that V and W are equally likely and independent.

Lemma 1. *A TRNG with a quantum photonic source as depicted in Fig. 2 and a composite extractor function $Ext(X, Y; r) = Ext_2(X)||Ext_r(Y; r)$ yields generated values that are uniformly distributed when $Ext_2(X)$ produces a uniformly distributed RV V and $Ext_r(Y)$ produces a uniformly distributed RV W.*

Proof. The probability that a variate of V is a value in the set $\mathbb{F}_2 = \{0, 1\}$ is $\frac{1}{2}$ since V is uniformly, or in this case, Bernoulli distributed with probability of success $\frac{1}{2}$. Likewise, the probability that a variate of RV W is a value in the set $\mathbb{F}_r$ is $\frac{1}{2^r}$ since W is also uniformly distributed. Since RVs V and W are independent, the probability of the $r + 1$ bit concatenated variate of RV S, or $s_i = v_i||w_i$ is $P[V||W] = P[X \cap Y] = P[X]P[Y] = \frac{1}{2^{r+1}}$.

3 TRNG Theory and Analysis

The detection of photons by either SPAD-0 or SPAD-1 is theoretically modeled as a sequence of events corresponding to observations of a Bernoulli-distributed random variable (RV), X, with parameter p. In the theoretically ideal case, the Hadamard operator is implemented with a perfect 50:50 beam splitter resulting in the Bernoulli PMF parameter p being exactly $\frac{1}{2}$. However, as discussed in a later section, perfectly ideal beam splitters are not realizable in the laboratory or in manufacturing environments. Thus, an extractor function is used to adjust for practical tolerances in actual beam splitters.

We model the output of a SPAD as the function f_{SPAD} that has a nominal output of 0V. Upon detecting a photon at time t, f_{SPAD} produces a rising edge of a short duration pulse where the constant T_{SPAD} represents the short pulsewidth characteristic of the SPAD and $u(t)$ represents a unit step function. The SPAD characteristic behavior as modeled by f_{SPAD} is $f_{SPAD}(t) = u(t) - u(t - T_{SPAD})$ when SPAD-T detects an idler photon at time t.

In considering the case of an ideal beamsplitter, the quantum state of the location-encoded photon is maximally superimposed and is of the form $|\phi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ since the parameter p in a Bernoulli probability density function is $\frac{1}{2}$. This results in a photon detection event that is equally likely to happen in either SPAD-0 or SPAD-1 with probability of occurance equal to $\frac{1}{2}$ in response to the production of a signal and idler pair from the SPDC. However, in terms of actual implementations of beam splitters, such an ideal case is never achieved in practice since the devices are fabricated within tolerance levels and may also suffer from other imperfections. Thus the TRNG with an architecture such as that in shown in Fig. 2 is more realistically modeled with the parameter p being of the form $p \neq \frac{1}{2}$. For this reason, we employ the use of the well-known von Neumann extractor function for $Ext_2(X)$ although other previously known extractors such as the Trevisan or Toeplitz Hashing approach may be used depending upon the intended application of the TRNG. For the purpose of this paper, the choice of the particular extractor used for this portion of the circuit is not relevant to the main contribution. Extractor $Ext_2(X)$ produces the extracted sequence of variates v_i from the extracted RV V.

The sequence of measured time intervals between photon detection events is representative of a sub-Poissonian process and is denoted by RV Y [1][7][19]. The variates y_i of RV Y are discretized values representing each interval Δt_i. The detection coincidence window values, T_{win}, are chosen and used in the FPGA (or CPU software) in regard to the SPS parameters to ensure that the time intervals between detection pulses from SPAD-T are indeed sub-Poissonian distributed thus minimizing photon number bunching within a measurement interval.

The actual $\Delta t_i \in \mathbb{R}$ time intervals are positive, real, and non-zero. Due to the fact that the TRNG is implemented with a hybrid of photonic, analog, and digital electronic circuitry, the observation and measurement of RV Y results in a discrete positive integer-valued variate, y_i, from the interval $y_i \in [n_1, n_2]$. The integer-valued y_i measurement estimates the actual real-valued Δt_i value via the relationship $y_i = \lceil \Delta t_i \times \tau \rceil$ where τ is the clock period of a digital incrementor circuit or counter within the TRNG that counts the number of τ time intervals that elapse between adjacent photon detection events in time.

Fig. 3 contains a plot of the TRNG detector activations. The heralded detector output is indicated on the horizontal axis representing the SPAD-T detector when it detects the presence of an idler photon as shown via a tick mark labeled t_i. t_i is the time at which the SPAD-T detects an incident idler photon causing a rising edge of f_{SPAD}. The vertical axis is labeled with two events; the detection of a signal photon at either the SPAD-0 or SPAD-1 detector. Each black dot on the plot of Fig. 3 indicates whether the signal photon was detected by the SPAD-0 or SPAD-1 detector. Theoretically, the signal photon is equally likely to be detected at either the SPAD-0 or the SPAD-1 detector since it is placed into maximal and equal superposition due to the Hadamard operator realized as a beam splitter and the resulting extracted v_i value as shown in Fig. 2 .

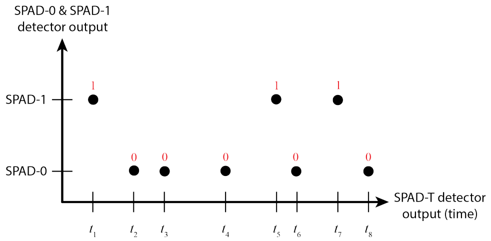

Fig. 3. Plot of time sequence of detected photon events by SPAD-0 and SPAD-1.

Fig. 3 actually indicates two statistically independent random processes. The first is modeled as RV V and is the equally likely event that the signal photon is detected by either the SPAD-0 or SPAD-1 detector. The second process, denoted as event RV X, corresponds to the event that the idler photon is detected by SPAD-T at some time interval Δt_i where $\Delta t_i = t_{i+1} - t_i$. Alternatively, the two sets of observations of RVs shown in Fig. 3 can be interpreted as the set of X observations, $\{1, 0, 0, 0, 1, 0, 1, 0\}$ and the set of Y observations $\{y_1, y_2, y_3, y_4, y_5, y_6, y_7\}$ are the discretized values representing $\{\Delta t_1, \Delta t_2, \Delta t_3, \Delta t_4, \Delta t_5, \Delta t_6, \Delta t_7\}$. In terms of information theory, each observation of X and Y yields some amount of self-information of the corresponding extracted values v_i and w_i, denoted as $I(v_i)$ and $I(w_i)$. The self-information, in units of bits, that corresponds to the event that RV A is observed to have an outcome of a_i (*i.e.* $A = a_i$) is given in Equation 1.

$$I(A = a_i) = -log_2[P(A = a_i)] \tag{1}$$

In the case of the information content of the strings resulting from the composite extractor function, $Ext(X, Y; r) = Ext_2(X)||Ext_r(Y; r)$, the TRNG provides a series of bit strings comprised of substrings, s_i, where s_i is the concatenation of the r-bit string w_i extracted from the y_i variates using extractor $Ext_r(Y;r) = w_i$, and the corresponding single bit values v_i extracted from variates x_i using the von Neumann extractor $v_i = Ext_2(X)$. Thus, the TRNG produces a series of substrings s_i that are comprised of $r+1$ bits formed as a concatenation $s_i = v_i||w_i$.

Lemma 2. *The concatenated string of $r+1$ bits, $s_i = v_i||w_i$, contains self information that is the arithmetic sum of the self information of v_i and w_i.*

Proof. From Lemma 1 it is proven that s_i, a variate of RV S, is uniformly distributed where $s_i = v_i||w_i$ and where v_i and w_i are each independent variates. Thus $P[s_i] = P[v_i||w_i] = P[v_i \cap w_i] = P[v_i]P[w_i] = P(v_i) \times P(w_i) = (\frac{1}{2})(\frac{1}{2^r}) = \frac{1}{2^{r+1}}$. Using the definition of self-information in Equation 1:

$$I(s_i) = -log_2[P(v_i) \times P[w_i] \quad = -log_2[P(v_i)] - log_2[P(w_i)] = I(v_i) + I(w_i)$$

For the ideal Hadamard operator in Fig. 3, the self-information due to an observation of RV X is, not surprisingly, one bit in the ideal case. For the RV W, the self-information due to the extracted value w_i is based on a substring of size r. Since the extracted w_i are ideally uniformly distributed, the self information is:

$$I(w_i) = -log_2[P(w_i)] = -log_2\left[\frac{1}{2^r}\right] = log_2(2^r) = r \qquad (2)$$

Information entropy is the expected value of the self-information, $H(A) = E\{I(A)\}$. Thus, for N_{tot} observations of A, assuming each A is comprised of k bits, the corresponding information entropy in units of bits is given in Equation 3.

$$H(A) = E\{I(A)\} = \sum_{i=1}^{k \times N_{tot}} I(A = a_i)P[I(A = a_i)] \qquad (3)$$

From probability theory, it is the case that $P[I(A = a_i)] = P[-log_2\{P(A = a_i)\}] = P[A = a_i]$, thus Equation 3 can be simplified to the well-known form in Equation 4.

$$H(A) = E\{I(A)\} = \sum_{i=1}^{k \times N_{tot}} P[a_i]log_2(P[a_i]) \qquad (4)$$

Theorem 1. *A TRNG with a quantum photonic source SPS as depicted in Fig. 2 and a composite extractor function $Ext(X,Y;r) = Ext_2(X)||Ext_r(Y;r)$ harvests more entropy from the SPS source than a TRNG that uses only the extractor $Ext_2(X)$ or only the extractor $Ext_r(Y;r)$.*

Proof. RV X and Y are statistically independent since the generation of photon pairs from the SPDC in the TRNG depicted in Fig. 2 occurs probabilistically and before the generated signal photon is placed into a state of superposition by the beamsplitter and subsequently detected by either SPAD-0 or SPAD-1. The N_{tot}-length sequence of $\{w_i\}$ is extracted from the N_{tot}-length sequence $\{y_i\}$ that are discretized values of $\{\Delta t_1, \Delta t_2, , \Delta t_{N_{tot}}\}$. While the N_{tot}-length sequence $\{y_i\}$ is a set of discretized sub-Poissonian distributed values of $\{\Delta t_1, \Delta t_2, , \Delta t_{N_{tot}}\}$, the corresponding $\{w_i\}$ sequence is a set of uniformly distributed length-r substrings due to extractor $Ext_r(Y; r)$ that are independent with regard to the signal photon being placed into a state of superposition prior to its detection by either SPAD-0 or SPAD-1. Alternatively, the outcome of the extracted v_i value from RV X is due to a fundamental axiom of quantum mechanics that is independent of the time intervals separating signal and idler pair generation from the SPDC.

The maximum amount of entropy available from a sequence of N_{tot} variates $\{v_i\}$ extracted from RV X occurs when the beam splitter is ideal and hence the von Neumann extractor has 100% efficiency and yields N_{tot} random bits when N_{tot} bits are operated over by the extractor. Thus, since each bit is equally likely to be zero or one, the resulting harvested entropy due to $Ext_2(X)$ is calculated on a per bit basis using Equation 4 resulting in Equation 5.

$$H(\{v_i\}) = -\sum_{i=1}^{1\times N_{tot}} P(v_i)log_2[P(v_i)] = -N_{tot}\left(\frac{1}{2}\right)log_2\left(\frac{1}{2}\right) = \frac{N_{tot}}{2} \tag{5}$$

Likewise, the entropy harvested from a sequence of N_{tot} substrings of length r, $\{w_i\}$, extracted from RV Y by $Ext_r(Y; r)$ is given by Equation 4 resulting in Equation 6.

$$H(\{w_i\}) = -\sum_{i=1}^{r\times N_{tot}} P(w_i)log_2[P(w_i)] = -(r\times N_{tot})\left(\frac{1}{2}\right)log_2\left(\frac{1}{2}\right) = \frac{N_{tot}}{2}(r) \tag{6}$$

Finally, the energy harvested from the sequence $\{s_i\}$ of length N_{tot} using the composite extractor $Ext(X, Y; r) = Ext_2(X)||Ext_r(Y; r)$ is given by Equation 4 resulting in Equation 7.

$$\begin{aligned} H(\{s_i\}) &= -\sum_{i=1}^{(r+1)\times N_{tot}} P(s_i)log_2[P(s_i)] = -\sum_{i=1}^{(r+1)\times N_{tot}} P(v_i||w_i)log_2[P(v_i||w_i)] \\ &= -\sum_{i=1}^{(r+1)\times N_{tot}} P(v_i\cap w_i)log_2[P(v_i\cap w_i)] = -\sum_{i=1}^{(r+1)\times N_{tot}} P(v_i)P(w_i)log_2[P(v_i)P(w_i)] \\ &= -\sum_{i=1}^{(r+1)\times N_{tot}} \left(\frac{1}{2}\right)\left(\frac{1}{2}\right)log_2\left[\left(\frac{1}{2}\right)\left(\frac{1}{2}\right)\right] = [(r+1)\times N_{tot}]\left(\frac{1}{2}\right) = \frac{N_{tot}}{2}(r+1) \end{aligned} \tag{7}$$

Comparing the entropy $H(\{s_i\})$ in Equation 7 with $H(\{v_i\})$ in Equation 5, we can calculate bounds on the value of r to ensure $H(\{s_i\}) > H(\{v_i\})$:

$$\frac{N_{tot}}{2}(r+1) > \frac{N_{tot}}{2} \implies r > 0$$

Thus, as long as $r > 1$, the entropy harvested from timing intervals w_i is larger than that from the state detection v_i and the proof is complete.

4 TRNG Implementation

A quantum photonic integrated circuit (QPIC) implementation of the TRNG architecture includes a Hadamard operator, implemented as a beam splitter, internally in the QPIC. The Hadamard operator is realized in a novel way by nanoscale frustrated total internal reflection (FTIR) couplers as shown in Fig. 4 [8][13][17][20]. This component comprises a thin trench that cuts across a waveguide at 45 degrees. This angle promotes total internal reflection (TIR) at the interface of the waveguide and the trench. If, however, the trench is etched thin enough so that a portion of the evanescent field is coupled into the subsequent waveguide, then the TIR is frustrated. To aid in fabrication and reliability, the etched trench is often backfilled by atomic layer deposition (ALD) with a low dielectric constant material. This component therefore allows an integrated realization of the macroscopic beamsplitter realization of a Hadamard gate. Fig. 4a depicts a schematic diagram of the arrangement of the integrated waveguides and the nanoscale FTIR coupler. Fig. 4b depicts a finite difference time domain (FDTD) simulation of photon tunneling into two perpendicular waveguides using a nanoscale FTIR coupler. A cross section of such a fabricated trench is shown in the scanning electron microscope (SEM) photograph of Fig. 4c, and a scanning electron microscope (SEM) photograph in Fig. 4d of a fabricated and functional nanoscale FTIR coupler.

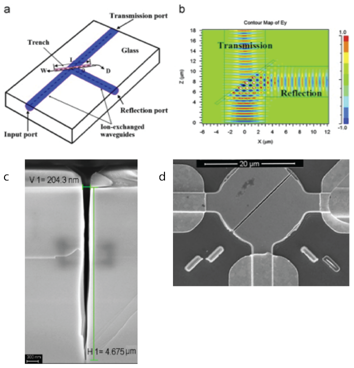

Fig. 4. Architecture, FDTD simulation, and scanning electron micro.

The FPGA, or alternatively an embedded CPU core, in Fig. 2 receives output from SPAD-T, SPAD-0, and SPAD-1. Internally the FPGA or CPU processing logic implements the extractor functions and produces a random bit stream as output in addition to other signal conditioning and control functions. Fig. 5 depicts a block diagram that partially illustrates the FPGA/CPU functionality of the proposed TRNG depicted in Fig. 2. This functionality is implemented as FPGA processing logic and/or as software in an embedded CPU core.

The parameters of the TRNG denoted as τ and R in Fig. 5 denote the internal sampling clock period (τ) that is smaller than the measurement coincidence window. The radix value, $R = 2^r$ is used to quantize the timing intervals Δt_i that yield the sub-Poissonian distributed variate $y_i \in [n_1, n_2]$. Each time a new idler photon is detected at SPAD-T, the fixed-point timer logic begins a processing cycle. The fixed-point timer logic (FPTL) computes $\Delta t_i = t_{i+1} - t_i$ as a quantized value in the form of an r-bit word y_i. The FPTL contains an internal incrementor register that is reset by a rising edge on the output of the SPAD-T detector and it is configured as an up-counter that increments every τ time units as a means to compute Δt_i. When an idler photon is detected by the SPAD-T, the incrementor first outputs its current discretized count value y_i to the extractor block labeled [TT:18] in Fig. 5, then it resets and begins counting again from zero. The output value of the incrementor is the quantized value of Δt_i representing an observation of RV Y for the previous time interval between photon detections with a resolution set by parameter τ. Note that y_i is not necessarily restricted to being r bits in length as is its extracted value, w_i.

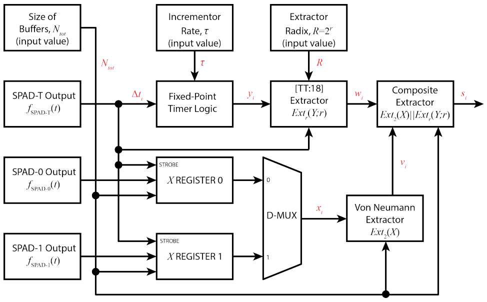
Size of Buffers, N_{tot} (input value)
Incrementor Rate, τ (input value)
Extractor Radix, $R=2^r$ (input value)
N_{tot}
τ
R
SPAD-T Output $f_{\text{SPAD-T}}(t)$
Δt_i
Fixed-Point Timer Logic
y_i
[TT:18] Extractor $Ext_r(Y;r)$
w_i
Composite Extractor $Ext_2(X)||Ext_r(Y;r)$
s_i
SPAD-0 Output $f_{\text{SPAD-0}}(t)$
STROBE
X REGISTER 0
0
D-MUX
x_i
v_i
Von Neumann Extractor $Ext_2(X)$
SPAD-1 Output $f_{\text{SPAD-1}}(t)$
STROBE
X REGISTER 1
1

Fig. 5. Block diagram of digital processing portion of the TRNG.

The block labeled [TT:18] Extractor implements the extractor function denoted as $Ext_r(Y; r)$ as described in [18]. It produces an r-bit value w_i whose value is in the set $\mathbb{F}_r = \{0, 1, , 2^{r-1}\}$ and that is uniformly distributed and produced from the input quantized y_i values derived from corresponding Δt_i values that are both sub-Poissonian distributed. This block also contains a buffer of a length suitable length to store N_{tot} different y_i and w_i sample values. The [TT:18] extractor block receives N_{tot} quantized y_i values, applies them to the $Ext_r(Y; r)$

function, and yields N_{tot} different w_i output values using the methodology described in [18]. The outputs of SPAD-0 and SPAD-1 are registered into single bit registers labeled “X Register 0” and “X Register 1” depending upon which SPAD outputs a pulse. The registers have values that are strobed in only when the SPAD-T rising edge occurs thus ensuring that the SPAD activations are due to an actual produced signal/idler pair from the SPDC versus some other spurious or extraneous detections. After an appropriate delay in the SPAD-T output signal (the delay element is not shown in Fig. 5) the demultiplexer logic outputs either a “0” or “1” electronic bit into the von Neumann extractor logic circuit depending on which of SPAD-0 or SPAD-1 was activated.

The von Neumann $Ext_2(X)$ extractor logic contains an internal buffer in the form of a serial input shift register that is also of length N_{tot}. When N_{tot} bits representing variates of RV X have been accumulated, the von Neumann extractor function evaluates thus ensuring that the samples, v_i, of RV V are indeed equiprobable. The block labeled “Composite Extractor” $Ext(X, Y; r) = Ext_2(X)||Ext_r(Y; r)$ receives the N_{tot} extracted bitstrings of length r, denoted as variates w_i, from the [18] $Ext_r(Y; r)$ block and the corresponding N_{tot} extracted bits from the von Neumann $Ext_2(X)$ extractor block. It then concatenates each r-bit value w_i with each matching single bit extracted value v_i and ideally outputs N_{tot} concatenated bit strings, $s_i = v_i||w_i$ each of length $r + 1$, as the TRNG output. Although we describe the composite extractor function $Ext(X, Y; r) = Ext_2(X)||Ext_r(Y; r)$ as performing concatenation resulting in random bit substrings of the form $s_i = v_i||w_i$, it is actually the case that the random bit v_i, can be inserted into any arbitrary location within the random bit string s_i without any degradation in terms of TRNG output quality.

5 Conclusion

A new TRNG architecture is presented that has enhanced throughput through the use of a new two-source extractor function that utilizes two sources of physical entropy from a single photonic source; a random sequence of time intervals and the randomness present in measurements of a superimposed quantum state. We also propose a novel structure that has been designed, fabricated, and tested in the QPIC of Fig. 4 that serves as the Hadamard operator for the purpose of transforming the quantum state of a signal photon into a superimposed state prior to its detection by either SPAD-0 or SPAD-1. This TRNG is suitable for implementation on a hybrid integrated circuit containing both photonic and electronic processing. The new extractor functions are implemented either within an on-chip FPGA or embedded electronic CPU core.

References

1. Arnoldus, H.F. and Nienhuis, G.: “Conditions for Sub-Poissonian Photon Statistics and Squeezed States in Resonance Fluorescence,” Optica Acta, 30(11):1573-1585 (1983).

2. Baetoniu, C.: “Method and Apparatus for True Random Number Generation,” U.S. Patent 7,389,316, June 17, 2008.
3. Dulz, W., Dulz, G., Hildebrandt, E., and Schmitzer, H. (inventors): “Method for Generating a Random Number on a Quantum-Mechanical Basis and Random Number Generator,” U.S. Patent 6,609,139, August 19, 2003.
4. Dorrendorf, L., Gutterman, Z., and Pinkas, B.: “Cryptanalysis of the random number generator of the Windows operating system,” ACM Transactions on Information and System Security 13(1) Article number 10, (2009).
5. Chattopadhyay, E.: “Explicit Two-source Extractors and More,” Ph.D. dissertation, The University of Texas at Austin, May 2016.
6. Chattopadhyay, E. and Zuckerman, D.: “Explicit Two-source Extractors and Resilient Functions,” in proc. ACM Symp. of the Theory of Computing (STOC), pp. 670-683, June 2016.
7. Fox, M.: Quantum Optics An Introduction, Oxford University Press, ISBN 13-978-0-19-856673-1, 2006.
8. Huntoon, N.R., Christensen, M.P., MacFarlane, D.L., Evans, G.A., and Yeh, C.S.: “Integrated Photonic Coupler Based on Frustrated Total Internal Reflection,” Applied Optics 47, 5682 (2008).
9. Hart, J.D., Terashima, Y., Uchida, A., Baumgartner, G.B., Murphy, T.E., and Roy, R.: “Recommendations and Illustrations for the Evaluation of Photonic Random Number Generators,” APL Photonics 2, 090901 (2017); https://doi.org/10.1063/1.5000056.
10. ID Quantique, SA: “Quantis Random Number Generator,” http://certesnetworks.com/pdf/alliance-solutions/QNRG-When-Randomness-Can-Not-Be-Left-To-Chance.pdf, (accessed November 16, 2018).
11. Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., and Zeilinger, A.: “A Fast and Compact Quantum Random Number Generator,” Review of Scientific Instruments, 71(4) 1675 (2000).
12. Koerner, B.: “Russians Engineer a Brilliant Slot Machine CheatAnd Casinos Have No Fix,” Wired Magazine Feb. 06, 2017.
13. Liu, K., Huang, H., Mu, S.X., Lin, H. and MacFarlane, D.L.: “Ultra-compact three-port trench-based photonic couplers in ion-exchanged glass waveguides,” Optics Communications 309, 307-312 (2013).
14. qutools GmbH: “Quantum Random Number Generator,” product datasheet, http://www.qutools.com/products/quRNG/quRNG_datasheet.pdf, (accessed June 9, 2018), 2010.
15. Shumow, D., Ferguson, N.: “On the Possibility of a Back Door in the NIST SP800-90 Dual EC,” http://rump2007.cr.yp.to/15-shumow.pdf.
16. Stipcevic, M.: “QBG121 Quantum Random Number Generator, Datasheet, v. 20060328,” http://www.irb.hr/users/stipcevi/index.html, (accessed June 9, 2018).
17. Sultana, N., Zhou, W., LaFave Jr., T.P., and MacFarlane, D.L.: “HBr Based ICP Etching of High Aspect Ratio Nanoscale Trenches in InP: Considerations for Photonic Applications,” J. Vac. Sci. Technol., B 27, 2351 (2009).
18. Thornton, M.A. and Thornton, M.A.: “Multiple-valued Random Digit Extraction,” in proc. IEEE Int. Symp. on Multiple-Valued Logic (ISMVL), pp. 162-167, May 2018.
19. Zou, X. and Mandel, L.: “Photon-antibunching and sub-Poissonian Photon Statistics,” Physical Review A, 41(1):475-476.
20. Zhou, W., Sultana, N., and MacFarlane, D.L.: “HBr-Based Inductively Coupled Plasma Etching of High Aspect Ratio Nanoscale Trenches in GaInAsP/InP,” J. Vac. Sci. Technol., B 26, 1896 (2008).