A Quantum Photonic TRNG based on Quaternary Logic

Kaitlin N. Smith[1], Duncan L. MacFarlane, and Mitchell A. Thornton
Department of Electrical and Computer Engineering
Southern Methodist University
Dallas, Texas, USA
{knsmith, dmacfarlane, mitch}@smu.edu

***Abstract*—An architecture for a quantum photonic true random number generator (TRNG) that takes advantage of higher-radix encoding schemes is presented. The TRNG is based upon two statistically independent sources of entropy: generated photon sequences at randomly distributed time intervals and the measurement of radix-4 superimposed quantum states. The two-source TRNG comprises of recently developed structures and extractor functions that enable it to be implemented in a quantum photonic integrated circuit (QPIC). We show that the amount of entropy extracted from the dual weakly random sources exceeds the amount of entropy that can be extracted from either of the single physical sources. We also describe several features of the TRNG architecture that enhance the data output rates.**

***Index Terms*—TRNG, QRNG, MVL, Extractor function, Photonic Integrated Circuit, Chrestenson**

I. Introduction

High-quality random number generators (RNG) are foundational building blocks for modern computer privacy and security applications. As the need for increased security is considered in combination with the explosive growth in ubiquitous embedded systems, RNGs that are compact, inexpensive, reliable, and are characterized by high output data rates are needed. The lack of high-quality random number sources in otherwise secure systems has been the cause of several well-documented security breaches [1]–[3].

RNGs are categorized as either pseudorandom number generators (PRNGs) or true random number generators (TRNGs). PRNGs produce periodic bit sequences of length N such that strings of size n, where $n < N$, have characteristics resembling those of a random string. Conversely, the class of TRNGs is based on a physical entropy source that has an inherent random nature. TRNGs are preferable in applications where security is of concern. Many sources of entropy have been identified and used in TRNGs, notably those based upon quantum effects.

The TRNG presented here is based upon quantum photonic effects and can be fabricated within a single photonic integrated circuit (PIC) for operation at room temperature. A unique aspect of our architecture is that two statistically independent entropy sources are combined to increase TRNG throughput. Due to the axioms of quantum mechanics wherein the measurement of an observable is probabilistic, the generation of a superimposed location-state coupled with a measurement mechanism serves as a physical entropy source [4]. Throughput is doubled via the use of radix-4 encoded photonic quantum states as compared to previous work that used binary encoded photonic quantum states [5].

The second source of entropy is based upon the probability that a pair of photons is produced when a single photon of higher frequency is incident upon a nonlinear medium. The effect of photon pair production is due to spontaneous parametric down conversion (SPDC) that is probabilistic and conserves energy by producing a photon pair whose total energy is equal to that of the incident photon. The SPDC-based entropy source results in a sequence of probabilistically-distributed intervals between SPDC photon pair production. We combine these two independent physical entropy sources to produce a single composite random digit stream with an increased output data rate.

Physical entropy sources used in TRNGs are often referred to as "weakly random sources" since it is difficult to measure the source output without adding some degree of determinism. Thus, an important aspect of TRNG design is the incorporation of an extractor function that transforms a weakly random source into a sequence that is ideally an equally likely and independent string of random digits. In the case of the TRNG architecture described here, it is necessary to employ a dual-source extractor that serves to combine the two weakly random entropy sources into a single output stream.

II. Quantum Photonic TRNG Architecture

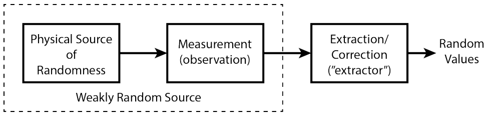
Physical Source of Randomness
Measurement (observation)
Extraction/ Correction ("extractor")
Random Values
Weakly Random Source

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

As shown in Fig. 1, TRNGs are generally comprised of a physical source of entropy, a measurement stage, and a post-measurement processing stage that contains an extractor function. We propose a TRNG implemented as a quantum photonic integrated circuit (QPIC) using location-encoded methods for

[1] K. N. Smith was with Southern Methodist University. She is now at the Department of Computer Science at the University of Chicago (email: kns@uchicago.edu).

information representation. This location-encoding is an extension of "dual-rail" radix-2 quantum computing, and is referred to as "quad-rail" as radix-4 logic is implemented.

The prototype TRNG is illustrated in Fig. 2. Here, a single photon pump excites a SPDC structure causing it to probabilistically generate a heralded single photon source (SPS) in the form of a signal and idler photon pair. The SPS is comprised of a pulsed laser source with wavelength 405 nm 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 SPDC. The down-converted signal and idler photons are at 810 nm wavelength. As is typical in a heralded photon system, the SPAD-T detector is used to indicate the presence of a down-converted photon pair by measuring the presence of the idler photon. We use the time intervals between subsequent SPAD-T output signals to serve as a weakly random entropy source since SPDC pair production is inherently probabilistic.

The signal photon is applied to a four-input, four-output radix-4 Chrestenson operator ($\mathbf{C}_4$) that places the photon, acting as an information carrier for a radix-4 qudit, into a state of maximal superposition [6], [7]. The $\mathbf{C}_4$ operator is implemented with a four-port directional coupler and has four ports that are encoded as $|0\rangle$, $|1\rangle$, $|2\rangle$, and $|3\rangle$. This component receives an input through the $|0\rangle$ terminal, and the superimposed output photon exits through one of the four output waveguides representing an orthogonal basis state in the set of $|0\rangle$, $|1\rangle$, $|2\rangle$, and $|3\rangle$. The idler photon is transmitted in a fifth waveguide that enables a heralded implementation. Each of the five waveguides drives a single-photon avalanche diode (SPAD) detector labeled as SPAD-0, SPAD-1, SPAD-2, SPAD-3, and SPAD-T. A random digit stream is produced depending upon which SPAD[0:3] device indicates light detection that is correlated with an active output from SPAD-T. This approach for implementing a TRNG using photonic quantum effects is well-known when used with binary basis states (*i.e.*, qubits) and a Hadamard operator. Variations of the binary approach are used in commercial devices [8]–[12]. Our approach, however, uses a radix-4 qudit in conjunction with a recently disclosed Chrestenson operator and also combines a second entropy source based on SPDC timing intervals to enhance overall data output rates.

A signal flow diagram that includes the four-port directional coupler is pictured in Fig. 3. The signal labeled as "Input 0" is first incident after the photon travels through a polarizing beam splitter and a half-wave plate. This causes the input signal and the output signal from the leftmost port of the coupler diagram to have orthogonal polarizations. The different polarizations of the input and output allow the output signal, labeled as "Output 0," to be coupled out of the device from the same port that the input signal, labeled "Input 0," is coupled into. When the four-port coupler is operated in a classical mode, a beam is incident into one of the coupler inputs causing it to route 25% of the incident beam to each of the four outputs. This beam division is caused by the transmission and reflection of signals within the coupler. Each fraction of the input beam observed

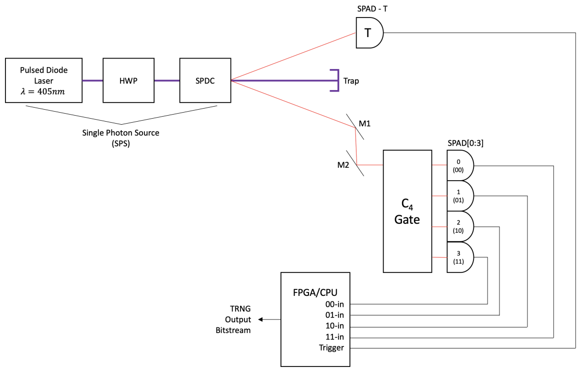

Fig. 2. A TRNG comprised of SPS, SPDC, and five SPADs.

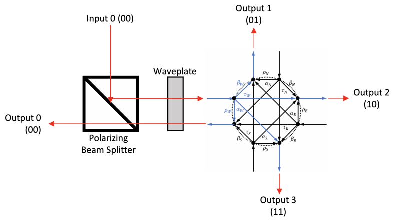

Fig. 3. Signal flow diagram of four-port directional coupler implementation of the $\mathbf{C}_4$ operator.

at an output corresponds to one of the following components of the original signal: a reflected component ρ, a transmitted component τ, a right-directed component α, and a left-directed component β. The four output beams of the directional coupler drive SPAD[0:3].

In order to operate the coupler in the quantum realm, the incident beam is reduced in intensity until only a single photon is emitted. In this case, only one of the four detectors, SPAD[0:3], will indicate the presence of output energy since the single photon is an indivisible energy packet. Furthermore, the particular SPAD detector that indicates the presence of energy is random and is equally likely for a device with equal reflection and transmission coefficients. Thus, in the quantum realm, the four-port coupler operates as a $\mathbf{C}_4$ gate. The combination of the $\mathbf{C}_4$ gate and the four SPAD[0:3] detectors serves as a weakly random source of entropy wherein the activation of SPAD[i] allows for the randomly generated radix-4 digit i to be generated.

The technique of using the polarizing beam splitter and half-wave plate to enable a single port to serve in a bidirectional manner is acceptable for a table-top prototype version of the proposed architecture. However, it is challenging to implement QPIC structures that are based upon polarization encoding. To implement the $\mathbf{C}_4$ operator within a QPIC, it is desirable to only use location-based encoding for the radix-4 qudit. Thus, an alternative structure may be used to implement the $\mathbf{C}_4$ gate in the QPIC that has a distinctly separate incident and output ports. By eliminating the bidirectional port in the $\mathbf{C}_4$ operator such as that shown in Fig. 3, we can eliminate the need for

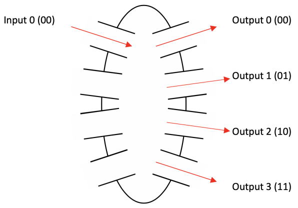

Fig. 4. Schematic of a photonic coupler cavity implementation of the $\mathbf{C}_4$ operator.

polarization encoding entirely. Such a structure is in the form of an array waveguide that is implemented with a photonic coupler cavity [13]. The schematic diagram for a cavity-based $\mathbf{C}_4$ gate is included in Fig. 4.

The architecture shown in Fig. 2 includes an FPGA or CPU core programmed to take advantage of two different random sources of entropy from the SPS. One source is a sequence of measurements based upon whether energy is detected at SPAD[0:3]. The other source is the sequence of time intervals between photon detection at any of the SPADs indicated by the output of the SPAD-T detector. These two outputs from the weakly random sources are modeled as random variables, RV, denoted as X that have values of $i \in \{0, 1, 2, 3\}$ when SPAD[i] indicates the presence of a photon, and RV Y that represents a time interval between subsequent SPDC pair production events. When the $\mathbf{C}_4$ operator and measurement SPADs are ideal, X is uniformly distributed and Y is a time series of sub-Poissonian distributed time intervals [14].

TRNGs can be improved when they are based upon two entropy sources as compared to a single source TRNG [15], [16]. However, appropriate two-source extractor functions must be used to realize the improvements. One of the purposes of the programmable element in our architecture is to host the two-source extractor function that transforms the weakly random sequences referred to as X and Y into a single extracted sequence that is close to uniform. Although Y is ideally a continuous RV, it is measured by way of an integrated high-speed digital counter with a finite register length of r. Each measured value of Y consists of r bits such that the variates of Y are values $y_i \in \{0, 1, \cdots, 2^r - 1\}$ that are distributed in a sub-Poissonian manner. The internal clock speed, register width r, and accuracy of the SPAD-T measurement dictate the entropy present in Y.

We use an extractor function, $Ext_r(Y; r)$, for the sub-Poissoinian distributed RV Y that was recently introduced in [17]. RV W is extracted from RV Y via $Ext_r(Y; r)$ and is of the form of a corresponding sequence of r-bit variates, w_i that are ideally uniformly distributed. The variates, y_i, of Y in our TRNG architecture are of the form of a discretized set of time intervals, Δt_i. The w_i values are radix-$R = 2^r$ 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 and is implemented in the FPGA or CPU core.

An extractor function $Ext(X)$ transforms the weakly random RV X into another RV denoted as V with a more uniform distribution. This extractor is needed due to imperfections in the $\mathbf{C}_4$ operator wherein the internal reflection and transmission coefficients may not be exactly equal. Considering the binary encoding of the radix-4 x_i variates, $\{00, 01, 10, 11\}$, and considering that a sequence of of x_i variates in this form result in a single bitstring that is weakly random, any of the well-known conventional binary extractor functions can be used.

Because X and Y are statistically independent, the composite extractor is formed from $Ext(X)$ and $Ext_r(Y; r)$ and is denoted as $S = V||W = Ext(X, Y; r) = Ext(X)||Ext_r(Y; r)$ where $||$ denotes the concatenation operation and S is the extracted composite RV from the two source extractor function, $Ext(X, Y; r)$. The choice of concatenating V with W is arbitrary. Generally, any arbitrary permutation of the bitstrings resulting from $s_i = v_i||w_i = Ext(x_i, y_i; r)$ would suffice.

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

Proof 1: The probability that a variate of V is a value in the set $\mathbb{F}_4 = \{00, 01, 10, 11\}$ is $\frac{1}{4}$ since V is uniformly distributed. 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 $r + 2$ bit concatenated variate of RV S, or $s_i = v_i||w_i$ is $P[V||W] = P[X \cap Y] = P[X]P[Y] = \frac{1}{2^{r+2}}$. □

III. Theory and Analysis

A SPAD is modeled as a function, f_{SPAD}, that has an output of 0V until the detection of a photon occurs at time t when f_{SPAD} produces a rising edge. 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. Here, $u(t)$ represents a unit step function and the constant T_{SPAD} represents the short pulsewidth characteristic of the SPAD. It is noted that the characteristic pulsewidth T_{SPAD} serves as a limiting factor for the parameter r, the size of the register that is used for y_i variate values.

Considering the case of an ideal four-port directional coupler, the state photon is maximally superimposed as $|\phi\rangle = \frac{|0\rangle+|1\rangle+|2\rangle+|3\rangle}{\sqrt{4}}$. Here, the probability that any of the four basis states $|i\rangle, i \in \{0, 1, 2, 3\}$ results from a measurement of energy present by SPAD[i] is $p = \frac{1}{4}$. Actual implementations of four-port couplers, however, do not achieve this exact equal probability distribution between output terminals. Therefore, the TRNG pictured in 2 produces the bits corresponding to the value of i for a measurement of $|i\rangle$ with $p \neq \frac{1}{4}$ in a realistic implementation. For this reason, we employ the use of an extractor function to cause the generated bits of the weakly random source denoted as RV X to yield RV

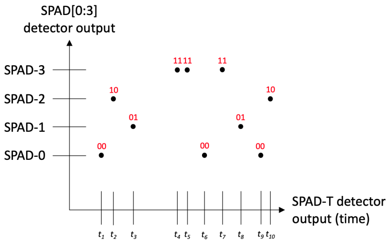

Fig. 5. Plot of time sequence of detected photon events by SPAD-0, SPAD-1, SPAD-2, and SPAD-3 at times t_i.

$V = Ext(X)$ that is uniformly distributed. Within this work, the von Neumann extractor is implemented as an example binary extractor function due to its simplicity. Higher efficiency binary extractors such as the Toeplitz hashing extractor or the Trevisan extractor can be used without loss of generality.

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 with respect 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 counter within the TRNG that counts the number of τ time intervals that elapse between adjacent photon detection events in time.

Fig. 5 contains a plot describing 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 four events: the detection of a signal photon at one of the SPAD[0:3] detectors.

Fig. 5 indicates two statistically independent random processes. The first is modeled as $RV\ X$ and is the equally likely event that the signal photon is detected by one of the SPAD[0:3] detectors. The second process, denoted as event $RV\ Y$, 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. 5 can be interpreted as the set of binary-encoded variates of $RV\ X$ observations, $\{00, 10, 01, 11, 11, 00, 11, 01, 00, 10\}$ and the set of observed variates of $RV\ Y$ observations $\{y_1, y_2, y_3, y_4, y_5, y_6, y_7\}$ that 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 Eqn. 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, $Ext(X, Y; r) = Ext(X)||Ext_r(Y; r)$, 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 bit pairs v_i extracted from variates x_i using the example binary extractor function, the von Neumann extractor, $v_i = Ext(X)$. Thus, the TRNG produces a series of substrings s_i that are comprised of $r + 2$ bits formed as a concatenation $s_i = v_i||w_i$.

Lemma 2: The concatenated string of $r+2$ 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 2: 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 $P[s_i] = P[v_i||w_i] = P[v_i \cap w_i] = P[v_i]P[w_i] = P(v_i) \times P(w_i) = (\frac{1}{4})(\frac{1}{2^r}) = \frac{1}{2^{r+2}}$. Using the definition of self-information in Eqn. 1:

$$\begin{aligned} I(s_i) &= -log_2[P(v_i) \times P(w_i)] = -log_2[P(v_i)] - log_2[P(w_i)] \\ &= I(v_i) + I(w_i) \end{aligned}$$

□

For the ideal radix-4 Chrestenson operator in Fig. 5, the self-information due to an observation of $RV\ X$ is two bits. 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:

$$\begin{aligned} I(w_i) = -log_2[P(w_i)] &= -log_2\left[\frac{1}{2^r}\right] \\ &= log_2(2^r) = r \end{aligned} \tag{2}$$

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 Eqn. 3.

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

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 Eqn. 3 can be simplified to the well-known form in Eqn. 4.

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

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

Proof 3: RVs X and Y are statistically independent 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.

The maximum amount of entropy available from a sequence of N_{tot} variates $\{v_i\}$, denoted as $H_{MAX}(V_{N_{tot}})$, is extracted from RV X when the four-port directional coupler is ideal and the von Neumann extractor has 100% efficiency and yields $2 \times N_{tot}$ random bits when N_{tot} SPAD[0:3] detection events are processed by $Ext(X)$. Thus, the entropy due to $Ext(X)$ is calculated on a per bit basis using Eqn. 4 resulting in Eqn. 5. Note that we define a particular variate v_i to be represented as the bitstring $b_1 b_0$ where each $b_j \in \{0, 1\}$. Because the maximum amount of entropy is an upper bound that assumes $Ext(X)$ results in an ideal uniform distribution of bits, $P(b_j) = \frac{1}{2}$ for all $j \in \{0, 1\}$.

$$\begin{aligned} H_{MAX}(V_{N_{tot}}) &= \sum_{i=1}^{N_{tot}} \left[- \sum_{j=0}^{1} P(b_j) log_2 [P(b_j)] \right] = \sum_{i=1}^{N_{tot}} \left[- \sum_{j=0}^{1} \left(\frac{1}{2}\right) log_2 \left(\frac{1}{2}\right) \right] \\ &= \sum_{i=1}^{N_{tot}} \left[\sum_{j=0}^{1} \left(\frac{1}{2}\right) \right] = N_{tot} \end{aligned} \tag{5}$$

Likewise, the maximum entropy harvested from a sequence of N_{tot} observed w_i substrings of length r, extracted from RV Y by $Ext_r(Y; r)$ is denoted by $H_{MAX}(W_{N_{tot}})$ and is given by Eqn. 4 resulting in Eqn. 6. Each variate w_i to be represented as the bitstring $c_{r-1} c_{r-2} \cdots c_0$ where $c_k \in \{0, 1\}$. Because the maximum amount of entropy is an upper bound that assumes $Ext(Y)$ results in an ideal uniform distribution of bits, $P(c_k) = \frac{1}{2}$ for all $k \in \{0, 1, \cdots, r-1\}$.

$$\begin{aligned} H_{MAX}(W_{N_{tot}}) &= \sum_{i=1}^{N_{tot}} \left[- \sum_{k=0}^{r-1} P(c_k) log_2 [P(c_k)] \right] = \sum_{i=1}^{N_{tot}} \left[- \sum_{k=0}^{r-1} \left(\frac{1}{2}\right) log_2 \left(\frac{1}{2}\right) \right] \\ &= \sum_{i=1}^{N_{tot}} \left[\sum_{k=0}^{r-1} \left(\frac{1}{2}\right) \right] = \frac{N_{tot}}{2} (r) \end{aligned} \tag{6}$$

Finally, the maximum entropy harvested from the sequence of N_{tot} extracted substrings $\{s_i\}$ of length $r+2$ using the composite extractor $S = Ext(X, Y; r) = Ext(X)||Ext_r(Y; r)$ is given by Eqn. 4 resulting in Eqn. 7 as $H_{MAX}(S_{N_{tot}})$. Note that we define a particular variate s_i to be represented as the $(r + 2)$-length bitstring $v_i||w_i = b_1 b_0 c_{r-1} c_{r-2} \cdots c_0$ where each $b_j, c_k \in \{0, 1\}$. Because the maximum amount of entropy is an upper bound that assumes $Ext(X, Y; r)$ results in an ideal uniform distribution of bits, $P(b_j) = P(c_k) = \frac{1}{2}$ for $j \in \{0, 1\}$ and $k \in \{0, 1, \cdots, r-1\}$.

$$\begin{aligned} H_{MAX}(S_{N_{tot}}) &= \sum_{i=1}^{N_{tot}} \left[- \sum_{j=0}^{1} P(b_j) log_2 [P(b_j)] - \sum_{k=0}^{r-1} P(c_k) log_2 [P(c_k)] \right] \\ &= - \sum_{i=1}^{N_{tot}} \left[\sum_{j=0}^{1} P(b_j) log_2 [P(b_j)] + \sum_{k=0}^{r-1} P(c_k) log_2 [P(c_k)] \right] \\ &= - \sum_{i=1}^{N_{tot}} \left[\sum_{j=0}^{1} \left(\frac{1}{2}\right) log_2 \left(\frac{1}{2}\right) + \sum_{k=0}^{r-1} \left(\frac{1}{2}\right) log_2 \left(\frac{1}{2}\right) \right] \\ &= - \sum_{i=1}^{N_{tot}} \left[- \sum_{j=0}^{1} \left(\frac{1}{2}\right) - \sum_{k=0}^{r-1} \left(\frac{1}{2}\right) \right] = \sum_{i=1}^{N_{tot}} \left[(1) + \left(\frac{r}{2}\right) \right] \\ &= \frac{N_{tot}}{2} (r + 2) \end{aligned} \tag{7}$$

Comparing the maximum entropy $H_{MAX}(S_{N_{tot}})$ in Eqn. 7 with $H_{MAX}(V_{N_{tot}})$ in Eqn. 5, we can calculate bounds on the value of r to ensure $H_{MAX}(S_{N_{tot}}) > H_{MAX}(V_{N_{tot}})$:

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

Likewise, comparing the entropy $H_{MAX}(S_{N_{tot}})$ in Eqn. 7 with $H_{MAX}(W_{N_{tot}})$ in Eqn. 6, we can calculate bounds on the value of r, the length of the substring w_i, to ensure $H_{MAX}(S_{N_{tot}}) > H_{MAX}(W_{N_{tot}})$:

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

Thus, as long as N_{tot} consists of at least one observation and the register size for the time interval measurements is at least one bit in width, the entropy harvested from the dual source TRNG proposed here is always greater than the entropy from a similar TRNG that uses only one random source alone.

□

IV. TRNG IMPLEMENTATION

A QPIC implementation of the TRNG architecture $\mathbf{C}_4$, implemented as a four-port directional coupler. The $\mathbf{C}_4$ is realized in a novel way by nanoscale frustrated total internal reflection (FTIR) couplers that intersect at a 90° angle [18], [19]. These couplers are comprised of thin trenches, backfilled with atomic layer deposition (ALD), that cut across a waveguide at 45° to promote total internal reflection (TIR) between the waveguide and trench.

The FPGA or CPU in Fig. 2 receives output from SPAD-T and SPAD[0:3]. Internally, the processing logic implements the extractor functions and produces a random bit stream as output in addition to other signal conditioning and control functions. Fig. 6 depicts a block diagram that partially illustrates the FPGA/CPU functionality of the proposed TRNG.

The parameters of the TRNG denoted as τ and R in Fig. 6 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 $y_i \in [n_1, n_2]$. The fixed-point timer logic (FPTL) begins a processing cycle at each detection at SPAD-T. The FPTL computes $\Delta t_i = t_{i+1} - t_i$ as a r-bit word y_i. The FPTL contains an internal incrementer register reset by each rising edge on the output of SPAD-T and is configured as an up-counter that increments every τ time

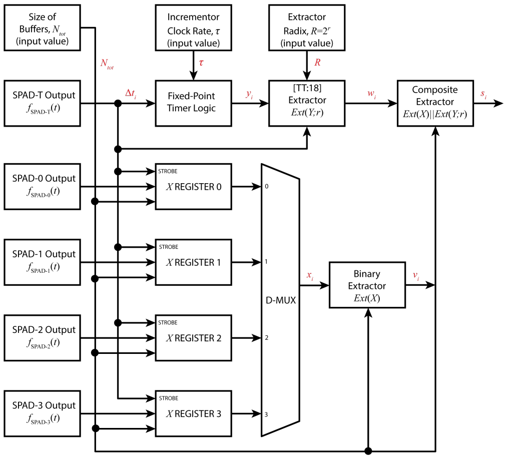

Fig. 6. Block diagram of digital processing portion of the TRNG.

units to compute Δt_i. When an idler photon is detected by the SPAD-T, the incrementer first outputs its current discretized count value y_i to the extractor block labeled [TT:18] in Fig. 6, then it resets and begins counting again from zero. The output value of the incrementer 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.

The block labeled [TT:18] implements the extractor function denoted as $Ext_r(Y;r)$ as described in [17]. It produces an r-bit value w_i whose value is in the set $\mathbb{F}_r = \{0, 1, ..., 2^{r-1}\}$ which 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 [17]. The outputs of SPAD[0:3] are stored in two-bit registers labeled register 0-3 depending upon the SPAD that outputs a pulse. The registers have values that are strobed in only when the SPAD-T rising edge occurs. After an appropriate delay in the SPAD-T output signal the demultiplexer logic outputs a bit pair of "00," "01," "10," or "11," depending on the activated SPAD.

The binary $Ext(X)$ extractor logic contains an internal buffer of length $2 \times N_{tot}$. When $2 \times N_{tot}$ bits representing variates of $RV\ X$ have been accumulated, the binary extractor function evaluates, ensuring that v_i of RV V are equiprobable. The composite extractor $Ext(X, Y; r) = Ext(X)||Ext(Y; r)$ receives the N_{tot} extracted bitstrings of length r, denoted as variates w_i, from the [17] $Ext(Y; r)$ block and the corresponding $2 \times N_{tot}$ extracted bits from the binary $Ext(X)$ function block. It then concatenates each r-bit value w_i with bit pairs v_i and ideally outputs N_{tot} concatenated bit strings, $s_i = v_i||w_i$, each of length $r + 2$.

V. Conclusion

A new TRNG architecture is presented that outputs high bandwith bitstreams through the implementation of a high-dimension quantum photonics element that places a quad-rail encoded photonic qudit in a state of equal and maximal superposition. Additionally, the TRNG extractor function incorporates an additional source of randomness through the analysis of the random sequence of photon pair generation times. This TRNG is suitable for implementation on an integrated circuit containing both photonic and electronic processing devices.

References

[1] L. Dorrendorf, Z. Gutterman, and B. Pinkas, "Cryptanalysis of the random number generator of the windows operating system," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 1, p. 10, 2009.

[2] B. Koerner, "Russians engineer a brilliant slot machine cheat—and casinos have no fix," *Wired*, 2017.

[3] D. Shumow and N. Ferguson, "On the possibility of a back door in the nist sp800-90 dual ec," http://rump2007.cr.yp.to/15-shumow.pdf.

[4] W. Dultz, G. Dultz, E. Hildebrandt, and H. Schmitzer, "Method for generating a random number on a quantum-mechanical basis and random number generator," Aug. 19 2003, uS Patent 6,609,139.

[5] M. A. Thornton and D. L. MacFarlane, "Quantum photonic trng with dual extractor," in *International Workshop on Quantum Technology and Optimization Problems*. Springer, 2019, pp. 171–182.

[6] K. N. Smith, T. P. LaFave, D. L. MacFarlane, and M. A. Thornton, "A radix-4 chrestenson gate for optical quantum computation," in *2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL)*. IEEE, 2018, pp. 260–265.

[7] K. N. Smith, T. P. LaFave Jr, D. L. MacFarlane, and M. A. Thornton, "Higher-radix chrestenson gates for photonic quantum computation," *JOURNAL OF APPLIED LOGICS-IFCOLOG JOURNAL OF LOGICS AND THEIR APPLICATIONS*, vol. 5, no. 9, pp. 1781–1798, 2018.

[8] C. Baetoniu, "Method and apparatus for true random number generation," Jun. 17 2008, uS Patent 7,389,316.

[9] "Quantis random number generator," http://certesnetworks.com/pdf/alliance-solutions/QNRG-When-Randomness-Can-Not-Be-Left-To-Chance.pdf, accessed: November 16, 2018.

[10] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, 2000.

[11] "Quantum random number generator," http://www.qutools.com/products/quRNG/quRNG_datasheet.pdf, accessed: June 9, 2018.

[12] M. Stipcevic, "Qbg121 quantum random number generator, datasheet, v. 20060328," http://www.irb.hr/users/stipcevi/index.html, accessed: June 9, 2018.

[13] L. B. Soldano and E. C. Pennings, "Optical multi-mode interference devices based on self-imaging: principles and applications," *Journal of lightwave technology*, vol. 13, no. 4, pp. 615–627, 1995.

[14] M. Fox, *Quantum optics: an introduction*. OUP Oxford, 2006, vol. 15.

[15] E. Chattopadhyay *et al.*, "Explicit two-source extractors and more," Ph.D. dissertation, University of Texas at Austin, 2016.

[16] E. Chattopadhyay and D. Zuckerman, "Explicit two-source extractors and resilient functions," in *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. ACM, 2016, pp. 670–683.

[17] M. Thornton and M. Thornton, "Multiple-valued random digit extraction," in *2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL)*. IEEE, 2018, pp. 162–167.

[18] D. L. MacFarlane, M. P. Christensen, K. Liu, T. P. LaFave, G. A. Evans, N. Sultana, T. Kim, J. Kim, J. B. Kirk, N. Huntoon *et al.*, "Four-port nanophotonic frustrated total internal reflection coupler," *IEEE Photonics Technology Letters*, vol. 24, no. 1, pp. 58–60, 2012.

[19] D. L. MacFarlane, M. P. Christensen, A. El Nagdi, G. A. Evans, L. R. Hunt, N. Huntoon, J. Kim, T. W. Kim, J. Kirk, T. P. LaFave *et al.*, "Experiment and theory of an active optical filter," *IEEE Journal of Quantum Electronics*, vol. 48, no. 3, pp. 307–317, 2012.