Stochastic performance analysis of a time-of-arrival quantum random number generator

Ágoston Schranz*†, Balázs Solymos*, Miklós Telek*†
*Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Hungary
†ELKH-BME Information Systems Research Group, Budapest, Hungary

***Abstract*—We present the performance analysis of the quantum random number generator (QRNG), reported in Ref. [1], operating based on the interarrival time differences between consecutive photon detections from a coherent light source. The proposed analysis approach accurately takes into account the physical properties of the single-photon detection systems, such as discretized time measurement, the correlations induced by the asynchronous arrival of photons with respect to the time resolution grid, and the dead time after observations and provides the QRNG's relevant performance measures, such as the joint distribution of bits, lag-r correlations, the bit generation overhead and the bit generation time. Analysis results are verified by computer simulations.**

***Index Terms*—Single-photon detection, quantum random number generation, Erlang distribution, mathematical analysis**

I. Introduction

Quantum random number generators have been the focal point of research for more than a decade now [2]. Such devices extract randomness from quantum physical phenomena, generating high-quality, non-deterministic sequences of uniformly distributed bits. Truly random sequences are essential in symmetric key cryptography, thereby in quantum key distribution (QKD) [3]. QRNGs may operate based on various physical effects, from which a large segment is of optical origin.

Optical time-of-arrival generators exploit the inherent randomness between photon arrival times from a coherent or thermal light source. These QRNGs provide simple methods for random number generation [1], [4]–[14], while relaxing the hardware requirements compared to generators adopting quasi-single-photon sources.

Generally, time-of-arrival generators can achieve bit generation rates around several Mbps, with some exceeding 100 Mbps [8], [12]. Specific methods generate bits that are uniform or close to uniform in distribution in their raw form. In contrast, others generate bits based on the underlying exponential distributions and apply different post-processing algorithms to whiten the bit sequences [15].

In our previous work [16], we developed the mathematical framework to analyze the bit generation efficiency and bit generation rate of the robust generator reported in Ref. [1] as a function of light intensity, detector dead time, and the precision of time measurement. However, we have settled for an assumption that majorly simplifies the analysis at the expense of general validity: the restartability of the measurement clock at each detection. In real-life devices and scenarios, this is often impossible or at least impractical—primarily if we aim for greater precision—and the clock is running continuously in the background. Its starting phase at each new interval depends on the previous random detection events, becoming a random variable. In this paper, we generalize our analysis, making it suitable for considering the correlation between consecutive samples obtained from discrete measurements of photon arrival instances.

The paper is organized as follows. Section II briefly describes the principle behind the random number generator's operation and introduces the notation. Section III details the analysis assuming that the measurement clock runs continuously, forming a deterministic grid. Unfortunately, the detailed analysis of the bit generation scheme becomes difficult with this deterministic approach, if the underlying samples are dependent. In order to overcome this obstacle, Section IV introduces an approximation using Erlang distributed grid times. Section V details the derivation of the joint distribution of bits based on the Erlang approximation, proving rigorously that the calculation of joint probabilities can be simplified significantly. The analysis is expanded with the effects of detector dead time in Section VI. Section VII introduces the relevant performance measures for the evaluation of the generation scheme (the joint distribution of bits, the lag-r correlations, the bit generation overhead, and the bit generation time), while Section VIII provides numerical results for these measures based on the Erlang approximation. Finally, Section IX concludes the paper and outlines the direction of related future research.

II. Principle of Operation

When classifying a device as a QRNG, it has to be evaluated carefully. It is desirable to prove that most entropy originates from a well-understood quantum effect rather than classical noise sources. Once that is ensured, analytical and simulation-based evaluation of the QRNG's properties is required before the generator is built.

Our generator operates based on a principle first described in Ref. [1], with only slight adjustments. A continuous-wave laser's light is attenuated to be suitably low. Throughout the paper, we assume that photons arrive according to a Poisson process with a constant rate λ. That is, the consecutive photon interarrival times are exponentially distributed with rate λ, and the photon arrivals are memoryless, i.e., from any point in time

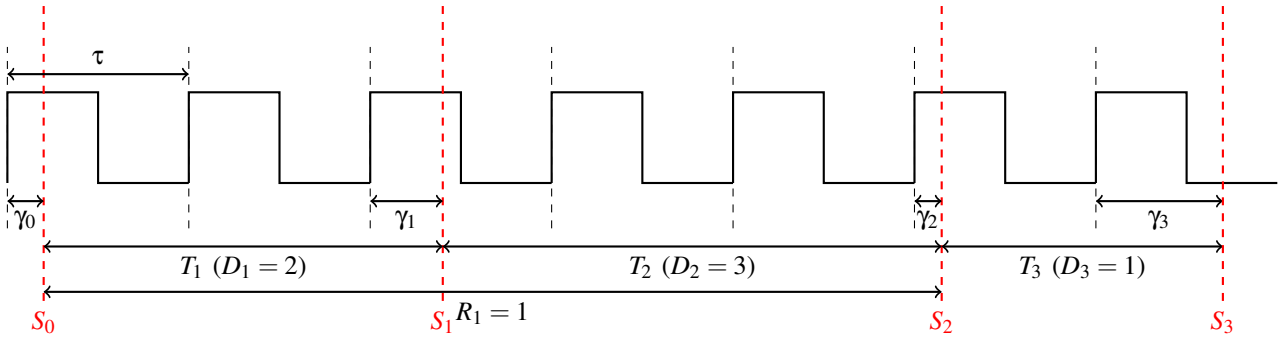

Figure 1. Photon arrivals and their measurements. Dashed black lines indicate the leading edges of the clock signals, whereas dashed red lines indicate photon arrivals.

(independent of future photon arrivals), the next photon arrives in an exponentially distributed amount of time, with rate λ.

The photons are detected by a single-photon detector, either a photomultiplier tube or a single-photon avalanche photodiode. We denote the photon arrival times by S_i and the time differences between them by $T_i = S_i - S_{i-1}$. The physical device measures the time differences between photon arrivals in clock units (denoted by τ) by counting a clock signal's leading edges between detections (D_i, see Fig. 1). In practice, we have access only to D_i, but not to T_i; thus, the QRNG is built on the discrete D_i samples.

The procedure described in Ref. [1] generates bits from the measured $D_1, D_2, \ldots$ samples as follows. If $D_{2i-1} > D_{2i}$, a zero bit is generated, if $D_{2i-1} < D_{2i}$ a bit 1 is generated. In case $D_{2i-1} = D_{2i}$, the D_{2i-1} and D_{2i} samples are dropped and no bit is generated.

For the analysis of the bit generation process, we formulate this procedure as follows. Subsequent measurements (D_{2i-1} and D_{2i}) are compared, and an R_i sequence is obtained as

$$R_i = \operatorname{sgn}(D_{2i} - D_{2i-1}) = \begin{cases} -1 & \text{if } D_{2i-1} > D_{2i}, \\ 0 & \text{if } D_{2i-1} = D_{2i}, \\ 1 & \text{if } D_{2i-1} < D_{2i}. \end{cases} \tag{1}$$

Let θ_n denote the nth non-zero element of the R_i sequence, and the ith bit is generated as

$$B_i = \begin{cases} 0 & \text{if } R_{\theta_i} = -1, \\ 1 & \text{if } R_{\theta_i} = 1. \end{cases} \tag{2}$$

III. Deterministic grid time

In this section, we analyze the observed samples' statistical properties, assuming that the deterministic grid time (the time measurement resolution) is τ and photons arrive according to a time-homogeneous Poisson process with rate λ.

A. Arrival instances on the grid

Let S_i be the time of the ith arrival of the Poisson process with parameter λ, $T_i = S_i - S_{i-1}$ the ith interarrival time and γ_i the time between S_i and its preceding τ grid border (c.f. Fig. 1). Consequently, $0 \le \gamma_i < \tau$. We refer to γ_i as the (continuous) phase variable as it describes the phase of the grid process at the ith photon arrival.

First, we investigate the distribution of γ_i. More precisely, we assume $\gamma_0 = x$ and compute the distribution of γ_1. For γ_1 we have

$$\gamma_1 = \tau \left\langle \frac{\gamma_0 + T}{\tau} \right\rangle, \tag{3}$$

where $\langle a \rangle = a - \lfloor a \rfloor$ is the fractional part of a, and the subscript of T_1 is suppressed for notational convenience. Based on this relation (for $0 \le x, y < \tau$), the conditional cumulative distribution function (CDF) of γ_1 is

$$\begin{aligned} F_{\gamma_1|\gamma_0=x}(y) &= \Pr(\gamma_1 < y \mid \gamma_0 = x) \\ &= \Pr(x + T < y) + \sum_{i=1}^{\infty} \Pr(i\tau \le x + T < i\tau + y) \\ &= \Pr\left(T < \max(y - x, 0)\right) + \sum_{i=1}^{\infty} \Pr(i\tau - x \le T < i\tau + y - x) \\ &= \chi_{\{y>x\}} \left(1 - \mathrm{e}^{-\lambda(y-x)}\right) \\ &\qquad + \sum_{i=1}^{\infty} \left[\left(1 - \mathrm{e}^{-\lambda(i\tau+y-x)}\right) - \left(1 - \mathrm{e}^{-\lambda(i\tau-x)}\right) \right] \\ &= \chi_{\{y>x\}} \left(1 - \mathrm{e}^{-\lambda(y-x)}\right) + \sum_{i=1}^{\infty} \left(\mathrm{e}^{-\lambda(i\tau-x)} - \mathrm{e}^{-\lambda(i\tau+y-x)}\right) \\ &= \chi_{\{y>x\}} \left(1 - \mathrm{e}^{-\lambda(y-x)}\right) + \mathrm{e}^{\lambda x} \left(1 - \mathrm{e}^{-\lambda y}\right) \sum_{i=1}^{\infty} \mathrm{e}^{-\lambda i\tau} \\ &= \chi_{\{y>x\}} \left(1 - \mathrm{e}^{-\lambda(y-x)}\right) + \mathrm{e}^{\lambda x} \left(1 - \mathrm{e}^{-\lambda y}\right) \frac{\mathrm{e}^{-\lambda\tau}}{1 - \mathrm{e}^{-\lambda\tau}}, \end{aligned} \tag{4}$$

where χ_A is the indicator of A, and we used the CDF of the exponential distribution with parameter λ, $\Pr(X < x) = 1 - \mathrm{e}^{-\lambda x}$. The conditional probability density function (PDF) of γ_1 (for $0 \le x, y < \tau$) is

$$\begin{aligned} f_{\gamma_1|\gamma_0=x}(y) &= \frac{\mathrm{d}}{\mathrm{d}y} F_{\gamma_1|\gamma_0=x}(y) \\ &= \chi_{\{y>x\}} \lambda \mathrm{e}^{-\lambda(y-x)} + \lambda \mathrm{e}^{-\lambda(y-x)} \frac{\mathrm{e}^{-\lambda\tau}}{1 - \mathrm{e}^{-\lambda\tau}}. \end{aligned} \tag{5}$$

First, we note that (5) depends on x, which means that the consecutive phase variables are *dependent*. Assuming that the distribution of γ_0 is known, the evolution of the random process $\gamma_0, \gamma_1, \ldots$ can be computed based on (5). The CDF and the PDF of the stationary phase at a photon arrival are defined as $F_\gamma(x) = \lim_{n\to\infty} \Pr(\gamma_n < x)$ and $f_\gamma(x) = \frac{\mathrm{d}}{\mathrm{d}x} F_\gamma(x)$.

Theorem 1. *The stationary phase at a photon arrival is uniformly distributed in* $[0,\tau)$.

Proof. The distribution of the stationary phase is associated with the eigenfunction of an operator composed from the characteristic function. Namely, $f_\gamma(\cdot)$ is the solution of

$$f_\gamma(y) = \int_{x=0}^{\tau} f_\gamma(x) f_{\gamma_1|\gamma_0=x}(y)\,\mathrm{d}x, \tag{6}$$

with normalization condition $\int_{y=0}^{\tau} f_\gamma(y)\mathrm{d}y = 1$. The solution of this integral equation is $f_\gamma(y) = \frac{1}{\tau}$ for $y \in [0,\tau)$, since

$$\begin{aligned} f_{\gamma_1|\gamma_0\equiv\text{uniform}}(y) &= \int_{x=0}^{\tau} \frac{1}{\tau} f_{\gamma_1|\gamma_0=x}(y)\,\mathrm{d}x \\ &= \int_{x=0}^{y} \frac{\lambda}{\tau}\mathrm{e}^{-\lambda(y-x)}\,\mathrm{d}x + \int_{x=0}^{\tau} \frac{\lambda}{\tau}\mathrm{e}^{-\lambda(y-x)}\frac{\mathrm{e}^{-\lambda\tau}}{1-\mathrm{e}^{-\lambda\tau}}\mathrm{d}x \\ &= \frac{\lambda}{\tau}\frac{1-\mathrm{e}^{-\lambda y}}{\lambda} + \frac{\lambda}{\tau}\frac{\mathrm{e}^{-\lambda y}(\mathrm{e}^{\lambda\tau}-1)}{\lambda}\frac{\mathrm{e}^{-\lambda\tau}}{1-\mathrm{e}^{-\lambda\tau}} = \frac{1}{\tau}. \end{aligned} \tag{7}$$

□

That is, if γ_0 is uniformly distributed on the τ grid, then every consecutive γ_i has a uniform marginal distribution.

The evolution of the random process $\gamma_0,\gamma_1,\ldots$ is important because the distribution of the observed variable D_i is determined by γ_{i-1}, as it is discussed in the next section.

B. Characteristic function of photon arrivals on the τ grid

Considering the phase variable, we investigate the distribution of $D_1, D_2, \ldots$. For $x,y \in [0,\tau)$ we write

$$\begin{aligned} F_n(x,y) &\triangleq \Pr(\gamma_1 < y, D_1 = n \mid \gamma_0 = x) \\ &= \begin{cases} \Pr(x+T<y) & \text{if } n=0, \\ \Pr(n\tau \le x+T < n\tau+y) & \text{if } n>0, \end{cases} \\ &= \begin{cases} \chi_{\{y>x\}}\left(1-\mathrm{e}^{-\lambda(y-x)}\right) & \text{if } n=0, \\ \mathrm{e}^{\lambda x}\left(1-\mathrm{e}^{-\lambda y}\right)\mathrm{e}^{-\lambda n\tau} & \text{if } n>0, \end{cases} \end{aligned} \tag{8}$$

and

$$\begin{aligned} f_n(x,y) &\triangleq \frac{\mathrm{d}}{\mathrm{d}y}\Pr(\gamma_1 < y, D_1 = n \mid \gamma_0 = x) \\ &= \begin{cases} \chi_{\{y>x\}}\lambda\mathrm{e}^{-\lambda(y-x)} & \text{if } n=0, \\ \lambda\mathrm{e}^{-\lambda(y+n\tau-x)} & \text{if } n>0. \end{cases} \end{aligned} \tag{9}$$

We refer to $f_n(x,y)$ as the characteristic function from which many performance indicators can be computed. E.g., the marginal distribution of γ_1 is

$$\begin{aligned} F_{\gamma_1|\gamma_0=x}(y) &= \Pr(\gamma_1 < y \mid \gamma_0 = x) = \sum_{n=0}^{\infty} F_n(x,y) \\ &= \chi_{\{y>x\}}\left(1-\mathrm{e}^{-\lambda(y-x)}\right) + \mathrm{e}^{\lambda x}\left(1-\mathrm{e}^{-\lambda y}\right)\frac{\mathrm{e}^{-\lambda\tau}}{1-\mathrm{e}^{-\lambda\tau}}. \end{aligned} \tag{10}$$

C. Distribution of the observed variables

The distribution of the observed variables, $D_1,\ldots,D_\ell$, can be obtained using the characteristic function. Focusing only on the first arrival and suppressing the related subscript, we have

$$\begin{aligned} \Pr(D = n \mid \gamma_0 = x_0) &= \int_{x_1=0}^{\tau} f_n(x_1,x_0)\,\mathrm{d}x_1 \\ &= \begin{cases} \Pr(x_0+T<\tau) & \text{if } n=0, \\ \Pr(n\tau \le x_0+T < (n+1)\tau) & \text{if } n>0, \end{cases} \\ &= \begin{cases} 1-\mathrm{e}^{-\lambda(\tau-x_0)} & \text{if } n=0, \\ \left(1-\mathrm{e}^{-\lambda\tau}\right)\mathrm{e}^{-\lambda(n\tau-x_0)} & \text{if } n>0. \end{cases} \end{aligned} \tag{11}$$

As the conditional distribution of the observation is given, the unconditional one is obtained by weighting with the stationary distribution of the phase γ, from which the marginal distribution of D is

$$\begin{aligned} \Pr(D=n) &= \int_{x_0=0}^{\tau} \frac{1}{\tau}\Pr(D=n \mid \gamma_0 = x_0)\,\mathrm{d}x_0 \\ &= \begin{cases} \int_{x_0=0}^{\tau} \frac{1}{\tau}\left(1-\mathrm{e}^{-\lambda(\tau-x_0)}\right)\mathrm{d}x_0 & \text{if } n=0, \\ \int_{x_0=0}^{\tau} \frac{1}{\tau}\left(1-\mathrm{e}^{-\lambda\tau}\right)\mathrm{e}^{-\lambda(n\tau-x_0)}\,\mathrm{d}x_0 & \text{if } n>0. \end{cases} \\ &= \begin{cases} 1-\frac{1-\mathrm{e}^{-\lambda\tau}}{\lambda\tau} & \text{if } n=0, \\ \mathrm{e}^{-\lambda\tau n}\frac{(1-\mathrm{e}^{-\lambda\tau})^2}{\lambda\tau\mathrm{e}^{-\lambda\tau}} & \text{if } n>0. \end{cases} \end{aligned} \tag{12}$$

This way, D is geometrically distributed with irregular initial probability, that is, $\Pr(D=n)$ form a geometric series from $n=1$ to infinity, but $\Pr(D=0)$ is different from the 0th element of that geometric series. We note that

$$\begin{aligned} \sum_{n=0}^{\infty}\Pr(D=n) &= 1 - \frac{1-\mathrm{e}^{-\lambda\tau}}{\lambda\tau} + \frac{(1-\mathrm{e}^{-\lambda\tau})^2}{\lambda\tau}\sum_{n=1}^{\infty}\mathrm{e}^{-\lambda\tau(n-1)} \\ &= 1 - \frac{1-\mathrm{e}^{-\lambda\tau}}{\lambda\tau} + \frac{(1-\mathrm{e}^{-\lambda\tau})^2}{\lambda\tau}\frac{1}{1-\mathrm{e}^{-\lambda\tau}} = 1 \end{aligned} \tag{13}$$

Similarly, the conditional joint distribution of $D_1,\ldots,D_\ell$ can be written as

$$\begin{aligned} &\Pr(D_1 = n_1,\ldots,D_\ell = n_\ell \mid \gamma_0 = x_0) \\ &= \int_{x_\ell=0}^{\tau}\cdots\int_{x_1=0}^{\tau}\prod_{m=1}^{\ell-1} f_{n_m}(x_{m-1},x_m)\,\mathrm{d}x_1\ldots\mathrm{d}x_\ell \end{aligned} \tag{14}$$

and the unconditional one as

$$\begin{aligned} &\Pr(D_1 = n_1,\ldots,D_\ell = n_\ell) \\ &= \int_{x_\ell=0}^{\tau}\cdots\int_{x_0=0}^{\tau}\frac{1}{\tau}\prod_{m=1}^{\ell-1} f_{n_m}(x_{m-1},x_m)\,\mathrm{d}x_0\ldots\mathrm{d}x_\ell. \end{aligned} \tag{15}$$

The last expression indicates that the $D_1,\ldots,D_\ell$ variables are correlated, making the generated bits correlated.

To simplify the notation of the stationary probabilities of bit sequences, we introduce $\mathrm{Bpr}(b_1,b_2,\ldots,b_{K-1},b_K) = \Pr(B_1=b_1,B_2=b_2,\ldots,B_{K-1}=b_{K-1},B_K=b_K)$.

Theorem 2. *For any bit sequence $b_1,\ldots,b_K$ of length K, the stationary probability of the K bit sequence satisfies*

$$\mathrm{Bpr}(b_1,b_2,\ldots,b_{K-1},b_K) = \mathrm{Bpr}(\bar{b}_K,\bar{b}_{K-1},\ldots,\bar{b}_2,\bar{b}_1), \tag{16}$$

where $\bar{b}_k$ denotes the inverse of b_k (if $b_k=1$ then $\bar{b}_k=0$ and vice versa).

We refer to (16) as the inverse-reverse relation. To prove the theorem, we need the following lemmas.

Lemma 1. *The inverse-reverse relation applies to the stationary behavior of the R_i series, that is*

$$\mathrm{Tpr}(r_1, r_2, \ldots, r_{K-1}, r_K) = \mathrm{Tpr}(\bar{r}_K, \bar{r}_{K-1}, \ldots, \bar{r}_2, \bar{r}_1), \qquad (17)$$

where $\mathrm{Tpr}(r_1, r_2, \ldots, r_K) = \Pr(R_1 = r_1, R_2 = r_2, \ldots, R_K = r_K)$ *and $\bar{r}_k$ denotes the inverse of r_k (such that $\bar{r}_k = -1$ if $r_k = 1$, $\bar{r}_k = 1$ if $r_k = -1$ and $\bar{r}_k = 0$ if $r_k = 0$).*

Proof. Let $T_1 = t_1, T_2 = t_2, \ldots, T_{2K} = t_{2K}$ be the photon interarrival times starting from a stationary arrival instance with γ_0, and let $\gamma_{2K} = \tau \left\langle \frac{\gamma_0 + \sum_{i=1}^{2K} T_i}{\tau} \right\rangle$ be the phase after the $2K$th photon arrival (c.f. Fig. 1).

Assuming that the associated discrete observations are $D_1 = d_1, D_2 = d_2, \ldots, D_{2K} = d_{2K}$ and $R_1 = r_1, R_2 = r_2, \ldots, R_K = r_K$, the probability density of the $T_1 = t_1, T_2 = t_2, \ldots, T_{2K} = t_{2K}$ samples which generates $R_1 = r_1, R_2 = r_2, \ldots, R_K = r_K$ is $\frac{1}{\tau} \prod_{i=1}^{2K} \lambda e^{-\lambda t_i}$, where we used that γ_0 is uniformly distributed in $[0, \tau)$ and T_i is exponentially distributed with parameter λ.

The photon interarrival sequence $T'_1 = t_{2K}, T'_2 = t_{2K-1}, \ldots, T'_{2K} = t_1$ starting from $\gamma'_0 = \tau - \gamma_{2K}$ results in the discrete observations $D'_1 = d_{2K}, D'_2 = d_{2K-1}, \ldots, D'_{2K} = d_1$ and $R'_1 = \bar{r}_K, R'_2 = \bar{r}_{K-1}, \ldots, R'_K = \bar{r}_1$, with probability density $\frac{1}{\tau} \prod_{i=1}^{2K} \lambda e^{-\lambda t_i}$, where we used that γ_{2K}, and consequently γ'_0, is uniformly distributed in $[0, \tau)$. That is, any trajectory of the Poisson arrival process has a trajectory with the same probability, which generates the inverse-reverse R_i series with the same probability. □

Lemma 2. *If* $\mathrm{Tpr}(r_1, r_2, \ldots, r_K) = \mathrm{Tpr}(\bar{r}_K, \bar{r}_{K-1}, \ldots, \bar{r}_1)$*, then* $\mathrm{Bpr}(b_1, b_2, \ldots, b_N) = \mathrm{Bpr}(\bar{b}_N, \bar{b}_{N-1}, \ldots, \bar{b}_1)$*, where N is the number of non-zero elements in the $r_1, r_2, \ldots, r_K$ series.*

Proof. The number of non-zero elements in $\bar{r}_K, \bar{r}_{K-1}, \ldots, \bar{r}_1$ is also N according to (2). The statement follows from the fact that the inverse relation of the non-zero R_{θ_i} elements implies the inverse relation of the associated D_i bits according to (2). □

Lemmas 1 and 2 imply Theorem 2.

Some direct consequences of Theorem 2 are $\mathrm{Bpr}(0) = \mathrm{Bpr}(1)$, $\mathrm{Bpr}(00) = \mathrm{Bpr}(11)$. Noting that $\mathrm{Bpr}(01) + \mathrm{Bpr}(11) = \mathrm{Bpr}(1)$ and $\mathrm{Bpr}(00) + \mathrm{Bpr}(10) = \mathrm{Bpr}(0)$, we also have

$$\mathrm{Bpr}(01) = \mathrm{Bpr}(1) - \mathrm{Bpr}(11) = \mathrm{Bpr}(0) - \mathrm{Bpr}(00) = \mathrm{Bpr}(10).$$

In a similar manner, according to Theorem 2 $\mathrm{Bpr}(000) = \mathrm{Bpr}(111)$, $\mathrm{Bpr}(001) = \mathrm{Bpr}(011)$, $\mathrm{Bpr}(010) = \mathrm{Bpr}(101)$, $\mathrm{Bpr}(100) = \mathrm{Bpr}(110)$ and additionally

$$\begin{aligned}\mathrm{Bpr}(011) &= \mathrm{Bpr}(11) - \mathrm{Bpr}(111) \\ &= \mathrm{Bpr}(00) - \mathrm{Bpr}(000) = \mathrm{Bpr}(100).\end{aligned}$$

That is, out of the 4 bit pair probabilities there are at most 2 different ones, and out of the 8 possible bit triple probabilities there are at most 3 different ones. For bit pairs and bit triples the bit tuples containing the same number of $0 \to 1$ and $1 \to 0$ transitions have the same probability. Unfortunately, Theorem 2 and the law of total probability does not ensure this property for higher bit tuples.

The analytical approach applied so far is efficient in computing the performance measures of the bit generation process if the D_i samples are independent. Unfortunately, the case when the samples are dependent is much harder to analyze with this approach. We introduce an analysis based on a stochastic approximation of the deterministic grid time τ to overcome this limitation.

IV. Erlang distributed grid times

Many stochastic models with deterministic time intervals are difficult to analyze. In such cases, it is a commonly applied technique to replace the deterministic time with a random time interval, whose presence makes the model easier to evaluate [17], [18]. When the random time closely approximates the deterministic time, i.e., the CDF of the random variable tends to the unit step function, the model's behavior with the random time tends to the model's behavior with the deterministic time.

The family of Erlang distributions is a family of distributions whose CDF tends to the unit step function. The CDF of the order N Erlang distribution with parameter μ, $1 - \sum_{n=0}^{N} (\mu x)^N e^{-\mu x} / N!$, tends to the unit step function as N tends to infinity and μ is proportional to $1/N$.

A. Arrival instances on the Erlang(μ,N) grid

Consider the Erlang(μ, N) distributed grids with $\mu = N/\tau$. We interpret the Erlang(μ, N) distributed grid time as the sum of N i.i.d exponentially distributed random time intervals with parameter μ and refer to those intervals as (discrete) phases. The Erlang(μ, N) distributed grid time is thus composed of N phases, and $J_i \in \{1, \ldots, N\}$ denotes the phase of the grid process at S_i. I.e., $J_i = 2$, if the ith photon arrival at S_i occurs in the second exponentially distributed period of the current grid.

For an exponentially distributed time interval with parameter λ, the number of phase changes in the grid process is geometrically distributed with parameter $p = \lambda/(\lambda + \mu)$, i.e, $\Pr(\Omega = k) = p(1-p)^k$, where Ω denotes the number of phase changes.

B. Distribution of the observed variables

Let D_i be the number of Erlang(μ, N) grids between S_{i-1} and S_i. To investigate the properties of the $D_1, D_2, \ldots$ process, for $i, j \in \{1, \ldots, N\}$, $n \geq 0$ we defined the size $N \times N$ matrices $\mathbf{A}_n$ whose elements are

$$\begin{aligned}\{\mathbf{A}_n\}_{ij} &= \Pr(J_1 = j, D_1 = n \mid J_0 = i) \\ &= \begin{cases} \Pr(\Omega = nN + j - i) & \text{if } nN + j \geq i, \\ 0 & \text{otherwise,} \end{cases} \\ &= \begin{cases} p(1-p)^{nN+j-i} & \text{if } nN + j \geq i, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \qquad (18)$$

These characteristic matrices play the same role as the characteristic functions in (5), from which similar performance indicators can be computed. E.g.

$$\begin{aligned}\Pr(D_1 = n \mid J_0 = i) &= \sum_{j=1}^{N} \Pr(J_1 = j, D_1 = n \mid J_0 = i) \\ &= \mathbf{e}_i \mathbf{A}_n \mathbb{1} \end{aligned} \tag{19}$$

and

$$\begin{aligned}\Pr(J_1 = j \mid J_0 = i) &= \sum_{n=0}^{\infty} \Pr(J_1 = j, D_1 = n \mid J_0 = i) \\ &= \sum_{n=0}^{\infty} \mathbf{e}_i \mathbf{A}_n \mathbf{e}_j^T \end{aligned} \tag{20}$$

where $\mathbb{1}$ is the column vector of ones and $\mathbf{e}_i$ is the i^{th} unit row vector.

Based on this characteristic matrix, the joint distribution of $D_1, \ldots, D_\ell$, is

$$\Pr(D_1 = n_1, \ldots, D_\ell = n_\ell \mid \gamma_0 = i) = \mathbf{e}_i \prod_{m=1}^{\ell} \mathbf{A}_{n_m} \mathbb{1} \tag{21}$$

According to (18), the characteristic matrices have a regular structure:

$$\mathbf{A}_0 = \begin{bmatrix} p & p(1-p) & \ldots & p(1-p)^{N-1} \\ & p & \ldots & p(1-p)^{N-2} \\ & & \ddots & \vdots \\ & & & p \end{bmatrix}, \tag{22}$$

$$\begin{aligned}\mathbf{A}_1 &= \begin{bmatrix} p(1-p)^N & p(1-p)^{N+1} & \ldots & p(1-p)^{2N-1} \\ p(1-p)^{N-1} & p(1-p)^N & \ldots & p(1-p)^{2N-2} \\ \vdots & & \ddots & \vdots \\ p(1-p) & p(1-p)^2 & \ldots & p(1-p)^N \end{bmatrix} \\ &= p(1-p) \begin{bmatrix} (1-p)^{N-1} \\ (1-p)^{N-2} \\ \vdots \\ 1 \end{bmatrix} \begin{bmatrix} 1 & (1-p) & \ldots & (1-p)^{N-1} \end{bmatrix} \end{aligned} \tag{23}$$

and for $n \geq 1$ they satisfy

$$\mathbf{A}_n = (1-p)^{(n-1)N} \mathbf{A}_1 = q^{n-1} \mathbf{A}_1, \tag{24}$$

where $q = (1-p)^N$. By definition, the $\mathbf{A}_i$ matrices satisfy $\sum_{i=0}^{\infty} \mathbf{A}_i \mathbb{1} = \mathbb{1}$.

Indeed, $(D_1, J_1), (D_2, J_2), \ldots$ form a discrete-time Markov chain (DTMC), where D_2 depends on J_1, but it is independent of D_1 for a fixed J_1. Consequently, the consecutive D_i samples would have been independent if the consecutive J_i values were independent.

V. Joint distribution of the generated bits

Our analysis aims to investigate the properties of the random bits which are generated from the observed $D_1, \ldots, D_\ell$ variables according to the bit generation process summarized in Section II.

A. Analysis of the generated bits

Let $\mathbf{p}$ be the length N row vector representing the initial phase of the process at S_0. The ith element of vector $\mathbf{p}$ is $[\mathbf{p}]_i = \Pr(J_0 = i)$.

From the first two observations, D_1 and D_2, the probabilities characterizing the different bit generation cases are

$$\Pr(D_1 < D_2 \mid \mathbf{p}) = \mathbf{p} \sum_{n=0}^{\infty} \sum_{m=n+1}^{\infty} \mathbf{A}_n \mathbf{A}_m \mathbb{1}, \tag{25}$$

$$\Pr(D_1 = D_2 \mid \mathbf{p}) = \mathbf{p} \sum_{n=0}^{\infty} \mathbf{A}_n \mathbf{A}_n \mathbb{1}, \tag{26}$$

$$\Pr(D_1 > D_2 \mid \mathbf{p}) = \mathbf{p} \sum_{n=1}^{\infty} \sum_{m=0}^{n-1} \mathbf{A}_n \mathbf{A}_m \mathbb{1}, \tag{27}$$

where the conditioning on $\mathbf{p}$ abbreviates that the initial phase of the process (J_0) equals i with probability $[\mathbf{p}]_i$.

We define $\mathbf{R}_0$, $\mathbf{R}_1$ and $\mathbf{R}_{-1}$, the characteristic matrices associated with the case of identical samples, $D_1 = D_2$, increasing samples, $D_1 < D_2$, and decreasing samples, $D_1 > D_2$, as

$$\mathbf{R}_0 = \sum_{n=0}^{\infty} \mathbf{A}_n \mathbf{A}_n, \ \mathbf{R}_1 = \sum_{n=0}^{\infty} \sum_{m=n+1}^{\infty} \mathbf{A}_n \mathbf{A}_m, \ \mathbf{R}_{-1} = \sum_{n=1}^{\infty} \sum_{m=0}^{n-1} \mathbf{A}_n \mathbf{A}_m, \tag{28}$$

respectively. Utilizing the regular structure of the $\mathbf{A}_i$ matrices, we further have

$$\mathbf{R}_0 = \sum_{n=0}^{\infty} \mathbf{A}_n^2 = \mathbf{A}_0^2 + \sum_{n=1}^{\infty} \left(\mathbf{A}_1 q^{n-1}\right)^2 = \mathbf{A}_0^2 + \frac{1}{1-q^2} \mathbf{A}_1^2 \tag{29}$$

$$\begin{aligned}\mathbf{R}_1 &= \sum_{n=0}^{\infty} \mathbf{A}_n \sum_{m=n+1}^{\infty} \mathbf{A}_m = \sum_{n=0}^{\infty} \mathbf{A}_n \frac{q^n}{1-q} \mathbf{A}_1 \\ &= \frac{1}{1-q} \mathbf{A}_0 \mathbf{A}_1 + \sum_{n=1}^{\infty} \mathbf{A}_1 q^{n-1} \frac{q^n}{1-q} \mathbf{A}_1 \\ &= \frac{1}{1-q} \mathbf{A}_0 \mathbf{A}_1 + \sum_{n=1}^{\infty} (q^2)^{n-1} \frac{q}{1-q} \mathbf{A}_1^2 \\ &= \frac{1}{1-q} \mathbf{A}_0 \mathbf{A}_1 + \frac{q}{(1-q^2)(1-q)} \mathbf{A}_1^2 \\ &= \frac{1}{1-q} \left(\mathbf{A}_0 + \frac{q}{1-q^2} \mathbf{A}_1 \right) \mathbf{A}_1, \end{aligned} \tag{30}$$

$$\begin{aligned}\mathbf{R}_{-1} &= \sum_{n=1}^{\infty} \sum_{m=0}^{n-1} \mathbf{A}_n \mathbf{A}_m = \sum_{n=1}^{\infty} q^{n-1} \mathbf{A}_1 \left(\mathbf{A}_0 + \sum_{m=1}^{n-1} q^{m-1} \mathbf{A}_1 \right) \\ &= \frac{1}{1-q} \mathbf{A}_1 \mathbf{A}_0 + \sum_{n=1}^{\infty} \frac{q^{n-1}(1-q^{n-1})}{1-q} \mathbf{A}_1^2 \\ &= \frac{1}{1-q} \mathbf{A}_1 \mathbf{A}_0 + \frac{q}{(1-q^2)(1-q)} \mathbf{A}_1^2 \\ &= \frac{1}{1-q} \mathbf{A}_1 \left(\mathbf{A}_0 + \frac{q}{1-q^2} \mathbf{A}_1 \right). \end{aligned} \tag{31}$$

We note that these matrices satisfy

$$\begin{aligned}&(\mathbf{R}_0 + \mathbf{R}_1 + \mathbf{R}_{-1}) \mathbb{1} \\ &= \left(\mathbf{A}_0^2 + \frac{1}{1-q} (\mathbf{A}_0 \mathbf{A}_1 + \mathbf{A}_1 \mathbf{A}_0) + \frac{1}{(1-q)^2} \mathbf{A}_1^2 \right) \mathbb{1} = \mathbb{1}. \end{aligned} \tag{32}$$

That is, the characteristic matrices represent the probability of every possible outcome of the bit generation process based on D_1, D_2.

From $\mathbf{R}_0$, $\mathbf{R}_1$ and $\mathbf{R}_{-1}$ the characteristic matrices of the generation of 1 and 0 bits are obtained as

$$\mathbf{B}_1 = \hat{\mathbf{R}}\mathbf{R}_1 = \hat{\mathbf{R}} \sum_{n=0}^{\infty} \sum_{m=n+1}^{\infty} \mathbf{A}_n \mathbf{A}_m, \tag{33}$$

$$\mathbf{B}_0 = \hat{\mathbf{R}}\mathbf{R}_{-1} = \hat{\mathbf{R}} \sum_{n=1}^{\infty} \sum_{m=0}^{n-1} \mathbf{A}_n \mathbf{A}_m, \tag{34}$$

where

$$\hat{\mathbf{R}} = \sum_{n=0}^{\infty} \mathbf{R}_0^n = (\mathbf{I} - \mathbf{R}_0)^{-1}$$

describes the effect of the dropped identical samples.

Theorem 3. *The ranks of matrices $\mathbf{B}_0$ and $\mathbf{B}_1$ are equal to one and consequently, they can be composed as dyadic products.*

Proof. In practically interesting systems (e.g., $\lambda > 0$), the $\mathbf{R}_1$, $\mathbf{R}_{-1}$ and similarly, the $\mathbf{B}_1$, $\mathbf{B}_0$ matrices are non-zero, because bits can be generated with positive probability. That is, the ranks of $\mathbf{R}_1$, $\mathbf{R}_{-1}$, $\mathbf{B}_1$, and $\mathbf{B}_0$ are at least one.

For quadratic matrices, it is known that $\operatorname{rank}(\mathbf{M}_1\mathbf{M}_2) \leq \min(\operatorname{rank}(\mathbf{M}_1), \operatorname{rank}(\mathbf{M}_2))$, and according to (23), $\operatorname{rank}(\mathbf{A}_1) = 1$, as it can be written as a dyadic product of two vectors. Consequently, according to (30) and (31) $\operatorname{rank}(\mathbf{R}_1) \leq 1$ and $\operatorname{rank}(\mathbf{R}_{-1}) \leq 1$, because

$$\operatorname{rank}(\mathbf{R}_1) \leq \min\left(\underbrace{\operatorname{rank}(\mathbf{A}_1)}_{1}, \operatorname{rank}\left(\mathbf{A}_0 + \frac{q}{1-q^2}\mathbf{A}_1 \right) \right).$$

Similarly, we obtain the statement of the theorem from (34) and (33). □

From the $\mathbf{B}_0$ and $\mathbf{B}_1$ characteristic matrices of the bit generation, the bit, bit-pair, and bit-n-tuple probabilities can be computed as

$$\Pr(B = 0 \mid \mathbf{p}) = \mathbf{p}\mathbf{B}_0\mathbb{1}, \quad \Pr(B = 1 \mid \mathbf{p}) = \mathbf{p}\mathbf{B}_1\mathbb{1}, \tag{35}$$

$$\Pr(B_0B_1 = i_0i_1 \mid \mathbf{p}) = \mathbf{p}\mathbf{B}_i\mathbf{B}_j\mathbb{1}, \quad (i_0, i_1) \in \{0,1\}^2, \tag{36}$$

and

$$\Pr(B_0 \dots B_{n-1} = i_0 \dots i_{n-1} \mid \mathbf{p}) = \mathbf{p} \prod_{k=1}^{n-1} \mathbf{B}_{i_k} \mathbb{1}, \quad (i_0, \dots, i_{n-1}) \in \{0,1\}^n. \tag{37}$$

From the bit-triplet probabilities, for $(i,k) \in \{0,1\}^2$, we have

$$\begin{aligned} \Pr(B_0B_2 = ik \mid \mathbf{p}) &= \sum_{j=0}^{1} \Pr(B_0B_1B_2 = ijk \mid \mathbf{p}) \\ &= \sum_{j=0}^{1} \mathbf{p}\mathbf{B}_i\mathbf{B}_j\mathbf{B}_k\mathbb{1} = \mathbf{p}\mathbf{B}_i\mathbf{B}\mathbf{B}_k\mathbb{1}, \end{aligned} \tag{38}$$

where $\mathbf{B} = \mathbf{B}_0 + \mathbf{B}_1$. That is, matrix $\mathbf{B}$ describes the phase transition probabilities during a bit generation. Applying similar reasoning, the joint distribution of bits, which are r bits apart, is

$$\Pr(B_0B_r = ik \mid \mathbf{p}) = \mathbf{p}\mathbf{B}_i\mathbf{B}^{r-1}\mathbf{B}_k\mathbb{1}, \tag{39}$$

where $(i,k) \in \{0,1\}^2$.

The only unknown in these expressions is $\mathbf{p}$. Since we are interested in the stationary properties of the bit generation process, $\mathbf{p}$ should be the stationary phase distribution at the beginning of a bit generation.

B. Stationary phase distribution at the beginning of a bit generation

The computation of the phase distribution at the beginning of a bit generation is based on the phase transition matrix, which describes the phase transition during a bit generation, $\mathbf{B}$. The stationary phase distribution vector, $\mathbf{p}$—representing the phase of the arrival process at the beginning of a bit generation—is obtained from matrix $\mathbf{B}$ as the solution of the linear system of equations $\mathbf{p}\mathbf{B} = \mathbf{p}$ and $\mathbf{p}\mathbb{1} = 1$.

C. Stationary bit sequence probabilities

Theorem 4. *For any bit sequence of length K, $b_1, \dots, b_K$, the stationary probability of the sequence can be computed from a single scalar quantity C as*

$$\operatorname{Bpr}(b_1, b_2, \dots, b_{K-1}, b_K) = \frac{1}{2} \prod_{j=1}^{K-1} c_{b_j, b_{j+1}} \tag{40}$$

where $c_{00} = c_{11} = C$, $c_{01} = c_{10} = 1 - C$, and $C = 2\operatorname{Bpr}(0,0)$.

We prove the theorem by the following lemmas.

Lemma 3. *For any bit sequence of length K, $b_1, \dots, b_K$, the stationary probability of the K long bits series can be computed from 8 scalar quantities $(e_0, e_1, c_{00}, c_{01}, c_{10}, c_{11}, f_0, f_1)$ as*

$$\operatorname{Bpr}(b_1, b_2, \dots, b_{K-1}, b_K) = e_{b_1} \prod_{j=1}^{K-1} c_{b_j, b_{j+1}} f_{b_K} \tag{41}$$

where $e_i = \mathbf{p}\mathbf{u}_i$, $f_i = \mathbf{v}_i\mathbb{1}$ for $i \in \{0,1\}$, $c_{ij} = \mathbf{v}_i\mathbf{u}_j$ for $(i,j) \in \{0,1\}^2$ and $\mathbf{B}_i = \mathbf{u}_i\mathbf{v}_i$ (with column vector $\mathbf{u}_i$ and row vector $\mathbf{v}_i$) is the dyadic decomposition of $\mathbf{B}_i$ for $i \in \{0,1\}$.

E.g., $\operatorname{Bpr}(1,1,0,1) = \mathbf{p}\mathbf{B}_1\mathbf{B}_1\mathbf{B}_0\mathbf{B}_1\mathbb{1} = e_1c_{11}c_{10}c_{01}f_1$.

Proof.

$$\operatorname{Bpr}(b_1, b_2, \dots, b_{K-1}, b_K) = \mathbf{p} \prod_{j=1}^{K} \mathbf{U}_{b_j} \mathbb{1} = \mathbf{p} \prod_{j=1}^{K} \mathbf{u}_{b_j}\mathbf{v}_{b_j}\mathbb{1} \tag{42}$$

$$= \mathbf{p}\mathbf{u}_{b_1} \prod_{j=1}^{K-1} \mathbf{v}_{b_j}\mathbf{u}_{b_{j+1}}\mathbf{v}_{b_K}\mathbb{1} = e_{b_1} \prod_{j=1}^{K-1} c_{b_j, b_{j+1}} f_{b_K}. \tag{43}$$

□

Lemma 4. *The $c_{01}, c_{10}, c_{11}, f_0, f_1$ parameters can be computed from e_0, e_1, c_{00} based on the following relations:*

$$f_i = \frac{1}{2e_i}, \; c_{11} = c_{00}, \; c_{01} = \frac{e_1}{e_0}(1 - c_{00}), \; c_{10} = \frac{e_0}{e_1}(1 - c_{00}),$$

where $i \in \{0,1\}$.

Proof. From Theorem 2 we have that the generator is unbiased, $\mathrm{Bpr}(0)=\mathrm{Bpr}(1)$, and also that $\mathrm{Bpr}(0,0)=\mathrm{Bpr}(1,1)$. Additionally, using that $\mathrm{Bpr}(0)+\mathrm{Bpr}(1)=1$, for $i\in\{0,1\}$, we obtain

$$\mathrm{Bpr}(i)=e_i f_i=\frac{1}{2}. \tag{44}$$

For the c_{ij} parameters, we utilize the following relations: $\mathrm{Bpr}(0,0)=\mathrm{Bpr}(1,1)$, $\mathrm{Bpr}(0,0)+\mathrm{Bpr}(0,1)=1/2$ and $\mathrm{Bpr}(0,0)+\mathrm{Bpr}(1,0)=1/2$, respectively.

$$\begin{aligned}\mathrm{Bpr}(0,0)&=e_0c_{00}f_0=\frac{1}{2}c_{00}\\&=\mathrm{Bpr}(1,1)=e_1c_{11}f_1=\frac{1}{2}c_{11}\end{aligned} \tag{45}$$

$$\begin{aligned}&\mathrm{Bpr}(0,0)+\mathrm{Bpr}(0,1)=e_0c_{00}f_0+e_0c_{01}f_1\\&=\frac{1}{2}c_{00}+e_0c_{01}\frac{1}{2e_1}=\frac{1}{2}\end{aligned} \tag{46}$$

$$\begin{aligned}&\mathrm{Bpr}(0,0)+\mathrm{Bpr}(1,0)=e_0c_{00}f_0+e_1c_{10}f_0\\&=\frac{1}{2}c_{00}+e_1c_{10}\frac{1}{2e_0}=\frac{1}{2},\end{aligned} \tag{47}$$

which gives the statements of the lemma. □

Lemma 5. *With appropriate scaling, $e_0=e_1=1$ and the only free parameter determining all bit sequence probabilities is $\mathrm{Bpr}(0,0)=c_{00}/2$.*

Proof. $\mathrm{Bpr}(0,0)=c_{00}/2$ is provided in (45). For $i\in\{0,1\}$, $\mathbf{B}_i=\mathbf{u}_i\mathbf{v}_i$, the dyadic decomposition of $\mathbf{B}_i$ is not unique. Let s_i be a non-zero constant, then $\mathbf{B}_i=(s_i\mathbf{u}_i)(\frac{1}{s_i}\mathbf{v}_i)$ is also a dyadic decomposition of $\mathbf{B}_i$. Using the $(s_i\mathbf{u}_i)(\frac{1}{s_i}\mathbf{v}_i)$ decomposition of $\mathbf{B}_i$ and setting $s_i=\frac{1}{\mathbf{p}\mathbf{u}_i}$, we obtain $e_i=\mathbf{p}(s_i\mathbf{u}_i)=1$, $f_i=\frac{1}{2e_i}=\frac{1}{2}$ and

$$c_{ij}=\left(\frac{1}{s_i}\mathbf{v}_i\right)\left(s_j\mathbf{u}_j\right)=\left(\mathbf{p}\mathbf{u}_i\mathbf{v}_i\right)\left(\frac{1}{\mathbf{p}\mathbf{u}_j}\mathbf{u}_j\right)$$

for $(i,j)\in\{0,1\}^2$. Here $c_{ii}=\mathbf{v}_i\mathbf{u}_i=\mathrm{Trace}(\mathbf{B}_i)$ is independent of s_i. □

Corollary 1. *The stationary probability of the $b_1,\dots,b_K$ bit sequence depends only on the number of $0\to1$ or $1\to0$ transitions. In a bit sequence of length K, K different bit sequence probabilities can occur.*

Proof. The first statement is a direct consequence of Theorem 4. The second statement comes from the fact that the number of $0\to1$ or $1\to0$ transitions can be $0,1,\dots,K-1$ in a bit sequence of length K. □

VI. Dead time

In the previous sections, we assumed that the physical equipment could observe every photon arrival, including those arbitrarily close to each other. In real physical devices, the photon sensor is blocked after each observed photon for a ζ long interval, which is referred to as *dead time*. It means that if an observed photon arrival occurs at S_0, then all photons arriving between S_0 and $S_0+\zeta$ are not recognized by the photon sensor, and the next observed photon is going to be the one that arrives first after $S_0+\zeta$, as it is depicted in Fig. 2. In the mathematical model, we assume that the system drops arrivals of the Poisson process between S_0 and $S_0+\zeta$ without any additional effects (the dead time is non-extendable).

A. Bit generation with dead time on the τ grid

Assuming that $\zeta=k\tau+\delta$ is constant, where $k\in\mathbb{N}$ and $0\le\delta<\tau$, we can compute the characteristic function considering the dead time (a modified version of (9)) as follows:

$$\begin{aligned}&F_n(x_0,x_1)=\Pr(D_1=n,\gamma_1<x_1\mid\gamma_0=x_0)\\&=\begin{cases}0 & \text{if } n<k,\\ \Pr(x_0+T+\delta<x_1) & \text{if } n=k,\\ \Pr\left((n-k)\tau\le x_0+T+\delta<(n-k)\tau+x_1\right) & \text{if } n>k,\end{cases}\\&=\begin{cases}0 & \text{if } n<k,\\ \chi_{\{x_0+\delta<x_1\}}\left(1-\mathrm{e}^{-\lambda(x_1-x_0-\delta)}\right) & \text{if } n=k,\\ \chi_{\{\tau<x_0+\delta<x_1\}}\left(1-\mathrm{e}^{-\lambda(x_1-x_0-\delta)}\right)\\ \quad+\chi_{\{x_0+\delta<\tau\}}\mathrm{e}^{-\lambda(\tau-x_0-\delta)}\left(1-\mathrm{e}^{-\lambda x_1}\right) & \text{if } n=k+1,\\ \left(\mathrm{e}^{-\lambda((n-k)\tau-x_0-\delta)}\right)\left(1-\mathrm{e}^{-\lambda x_1}\right) & \text{if } n>k+1.\end{cases}\end{aligned} \tag{48}$$

The resulting measures of the bit generation process can be computed from this modified characteristic function as in Section III-C. E.g., the conditional distribution of D_1 is $F_n(x_0,\tau)=\Pr(D_1=n\mid\gamma_0=x_0)$ and the marginal distribution of D_1 assuming uniform initial phase distribution is

$$\begin{aligned}&p_n=\Pr(D_1=n)=\int_{x_0=0}^{\tau}\frac{1}{\tau}\Pr(D_1=n\mid\gamma_0=x_0)\,\mathrm{d}x_0\\&=\begin{cases}0 & \text{if } n<k,\\ \int_{x_0=0}^{\tau-\delta}\frac{1}{\tau}\left(1-\mathrm{e}^{-\lambda(\tau-x_0-\delta)}\right)\mathrm{d}x_0 & \text{if } n=k,\\ \int_{x_0=0}^{\tau-\delta}\frac{1}{\tau}\left(\mathrm{e}^{-\lambda(\tau-x_0-\delta)}\right)\left(1-\mathrm{e}^{-\lambda\tau}\right)\mathrm{d}x_0\\ \quad+\int_{x_0=\tau-\delta}^{\tau}\frac{1}{\tau}\left(1-\mathrm{e}^{-\lambda(2\tau-x_0-\delta)}\right)\mathrm{d}x_0 & \text{if } n=k+1,\\ \int_{x_0=0}^{\tau}\frac{1}{\tau}\left(1-\mathrm{e}^{-\lambda\tau}\right)\mathrm{e}^{-\lambda((n-k)\tau-x_0-\delta)}\,\mathrm{d}x_0 & \text{if } n>k+1.\end{cases}\\&=\begin{cases}0 & \text{if } n<k,\\ \frac{\mathrm{e}^{-\lambda(\tau-\delta)}+\lambda(\tau-\delta)-1}{\lambda\tau} & \text{if } n=k,\\ \frac{\mathrm{e}^{-2\lambda\tau}(\mathrm{e}^{\lambda\tau}-1)(\mathrm{e}^{\lambda\tau}-\mathrm{e}^{\lambda\delta})}{\lambda\tau}+\frac{\lambda\delta-(\mathrm{e}^{\lambda\delta}-1)\mathrm{e}^{-\lambda\tau}}{\lambda\tau} & \text{if } n=k+1,\\ \frac{(\mathrm{e}^{\lambda\tau}-1)^2\mathrm{e}^{\lambda(\delta-(n-k+1)\tau)}}{\lambda\tau} & \text{if } n>k+1.\end{cases}\end{aligned} \tag{49}$$

Corollary 2. *Theorem 2, i.e. the inverse-reverse relation defined in* (16)*, remains valid also in case of non-zero dead time.*

Proof. The proof of the corollary follows the same pattern as the proof of Theorem 2. □

In case of zero dead time, the importance of Theorem 2 is negligible, because Theorem 4 provides more information about the stationary bit probabilities, but in case of non-zero dead time, Corollary 2 has a special importance, because Theorem 4 does not hold in this case.

B. Bit generation with dead time on the Erlang distributed grid

In this model, we assume that the grid time is Erlang$(N/\tau,N)$ distributed, which is composed of N i.i.d. exponentially distributed phases with rate N/τ and the dead time is

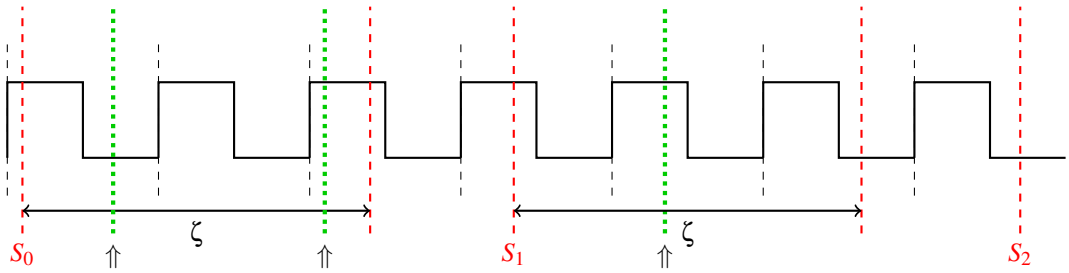

Figure 2. Photons, which arrive during the ζ long dead time following an observed photon arrival, are not observed. Non-observed photon arrivals are indicated by ⇑.

Erlang$(N/\tau, Z)$ distributed, which is composed of $Z = \zeta N/\tau$ i.i.d. exponentially distributed phases with rate N/τ, where $Z = kN + d$ is assumed to be an integer such that $0 \le d \le N-1$.

During the Z phases long dead time, the arrivals are dropped. By the dead time, the characteristic matrix of the process is the following modified version of (18)

$$\begin{aligned}\{\mathbf{A}_n\}_{ij} &= \Pr(J_1 = j, D_1 = n \mid J_0 = i) \qquad (50)\\ &= \begin{cases} \Pr(\Omega = nN + j - i - Z) & \text{if } nN + j \ge i + Z,\\ 0 & \text{otherwise,}\end{cases}\\ &= \begin{cases} p(1-p)^{nN+j-i-Z} & \text{if } nN + j \ge i + Z,\\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

Consequently, for $n < k$, $\mathbf{A}_n = \mathbf{0}$ and for $n \ge k+2$, we have

$$\mathbf{A}_n = (1-p)^{(n-k-2)N}\mathbf{A}_{k+2} = q^{n-k-2}\mathbf{A}_{k+2}, \qquad (51)$$

where $q = (1-p)^N$.

Using (51), for $\mathbf{R}_0$, $\mathbf{R}_1$, and $\mathbf{R}_{-1}$ we have

$$\begin{aligned}\mathbf{R}_0 &= \sum_{n=0}^{\infty}\mathbf{A}_n^2 = \mathbf{A}_k^2 + \mathbf{A}_{k+1}^2 + \sum_{n=2}^{\infty}\left(\mathbf{A}_{k+2}q^{n-2}\right)^2\\ &= \mathbf{A}_k^2 + \mathbf{A}_{k+1}^2 + \frac{1}{1-q^2}\mathbf{A}_{k+2}^2, \qquad (52)\end{aligned}$$

$$\begin{aligned}\mathbf{R}_1 &= \sum_{n=0}^{\infty}\mathbf{A}_n\sum_{m=n+1}^{\infty}\mathbf{A}_m = \qquad (53)\\ &= \mathbf{A}_k\left(\mathbf{A}_{k+1} + \frac{1}{1-q}\mathbf{A}_{k+2}\right) + \mathbf{A}_{k+1}\left(\frac{1}{1-q}\mathbf{A}_{k+2}\right)\\ &\qquad + \sum_{n=2}^{\infty}\mathbf{A}_n\left(\frac{q^{n-1}}{1-q}\mathbf{A}_{k+2}\right)\\ &= \mathbf{A}_k\left(\mathbf{A}_{k+1} + \frac{1}{1-q}\mathbf{A}_{k+2}\right) + \mathbf{A}_{k+1}\left(\frac{1}{1-q}\mathbf{A}_{k+2}\right)\\ &\qquad + \sum_{n=2}^{\infty}q^{n-2}\mathbf{A}_{k+2}\left(\frac{q^{n-1}}{1-q}\mathbf{A}_{k+2}\right)\\ &= \mathbf{A}_k\mathbf{A}_{k+1} + \frac{1}{1-q}(\mathbf{A}_k + \mathbf{A}_{k+1})\mathbf{A}_{k+2} + \frac{q}{(1-q^2)(1-q)}\mathbf{A}_{k+1}^2,\end{aligned}$$

$$\begin{aligned}\mathbf{R}_{-1} &= \sum_{n=1}^{\infty}\sum_{m=0}^{n-1}\mathbf{A}_n\mathbf{A}_m \qquad (54)\\ &= \mathbf{A}_{k+1}\mathbf{A}_k + \mathbf{A}_{k+2}(\mathbf{A}_k + \mathbf{A}_{k+1}) + \sum_{n=3}^{\infty}\mathbf{A}_n\left(\mathbf{A}_k + \mathbf{A}_{k+2} + \sum_{m=2}^{n-1}\mathbf{A}_m\right)\\ &= \mathbf{A}_{k+1}\mathbf{A}_k + \mathbf{A}_{k+2}(\mathbf{A}_k + \mathbf{A}_{k+1})\\ &\qquad + \sum_{n=3}^{\infty}q^{n-2}\mathbf{A}_{k+2}\left(\mathbf{A}_k + \mathbf{A}_{k+2} + \sum_{m=2}^{n-1}q^{m-2}\mathbf{A}_{k+2}\right)\\ &= \mathbf{A}_{k+1}\mathbf{A}_k + \frac{1}{1-q}\mathbf{A}_{k+2}(\mathbf{A}_k + \mathbf{A}_{k+1})\\ &\qquad + \sum_{n=3}^{\infty}q^{n-2}\mathbf{A}_{k+2}\frac{1-q^{n-2}}{1-q}\mathbf{A}_{k+2}\\ &= \mathbf{A}_{k+1}\mathbf{A}_k + \frac{1}{1-q}\mathbf{A}_{k+2}(\mathbf{A}_k + \mathbf{A}_{k+1}) + \frac{q}{(1-q^2)(1-q)}\mathbf{A}_{k+1}^2,\end{aligned}$$

which satisfies $(\mathbf{R}_0 + \mathbf{R}_1 + \mathbf{R}_{-1})\mathbb{1} = \mathbb{1}$.

Remark 1. *In this paper, we assume the dead time of the single-photon detection system to be deterministic. However, our analysis approach can be extended to a random dead time with a known distribution since* (50) *depends on Z. If Z is a random variable with distribution* $\Pr(Z = i) = \gamma_i$*, then* $\mathbf{A}_n$ *can be computed as* $\mathbf{A}_n = \sum_i \gamma_i \mathbf{A}_n(Z = i)$*, where* $\mathbf{A}_n(Z = i)$ *denotes the phase transition matrix assuming* $Z = i$ *and the same performance analysis can be applied based on the obtained* $\mathbf{A}_n$*.*

VII. Performance measures

As mentioned in Section III, the analysis approach based on the deterministic grid time has limitations in computing complex performance measures. This section summarizes the performance measures of interest and their computation based on the Erlang distributed grid time assumptions.

A. Joint distribution of bits

The bit, bit-pair, and bit-n-tuple probabilities can be computed from (35), (36) and (37), respectively, where, in case of non-zero dead time, the $\mathbf{R_0}$, $\mathbf{R_1}$, $\mathbf{R_{-1}}$ matrices are computed based on (52), (53),(54), respectively, using the modified characteristic matrix in (50).

B. Lag-r correlation

If X and Y are binary random variables with distributions $\Pr(X=i,Y=j)=p_{ij}$ (for $i,j\in\{0,1\}$), then their correlation is

$$C_{X,Y}=\frac{p_{11}-(p_{01}+p_{11})(p_{10}+p_{11})}{\sqrt{(p_{10}+p_{11})(1-p_{10}-p_{11})}} \times\frac{1}{\sqrt{(p_{01}+p_{11})(1-p_{01}-p_{11})}}, \tag{55}$$

since $E(X)=E(X^2)=p_{10}+p_{11}$ and $E(Y)=E(Y^2)=p_{01}+p_{11}$.

The lag-r correlation of the photon-generated bit sequence can be computed as C_{B_0,B_r}. For the lag-1 correlation, the required probabilities are provided in (36). For $r\geq 1$, the lag-r correlation can be computed based on (39).

C. Bit generation overhead

We define the bit generation overhead as the mean number of observed D_i variables (observed photons) needed to generate a bit. In the best case, when $D_1\neq D_2$, one bit is generated from two observed variables. To compute the average number of observed variables, we introduce random variable ρ as the number of observed variables needed to generate a bit. The distribution of ρ is

$$\Pr(\rho=2i)=\mathbf{p}\mathbf{R}_0^{i-1}(\mathbf{R}_1+\mathbf{R}_{-1})\mathbb{1}, \tag{56}$$

and its expected value is

$$\begin{aligned}E(\rho)&=\sum_{i=1}^{\infty}2i\mathbf{p}\mathbf{R}_0^{i-1}(\mathbf{R}_1+\mathbf{R}_{-1})\mathbb{1}\\&=2\mathbf{p}\left(\mathbf{I}-\mathbf{R}_0\right)^{-2}(\mathbf{R}_1+\mathbf{R}_{-1})\mathbb{1}.\end{aligned} \tag{57}$$

We note that only the observed photons are considered in ρ. Photons arriving during the dead time does not affect ρ. The next measure considers also the dead time.

D. Bit generation time

We define the bit generation time as the mean time for generating a single bit. To compute the bit generation time, we count the elapsed number of exponentially distributed phases during the bit generation process. According to the Erlang distributed grid time, we measure the time between photon arrivals in phase increments, where a grid interval is composed of N phases. Let Θ_i be the phase increment during the ith photon interarrival time, and we define the time-dependent kernel matrix for $t\geq 0$ as

$$\begin{aligned}\{\bar{\mathbf{A}}_n\}_{ij}(t)&=\Pr(J_1=j,D_1=n,\Theta_1=t\mid J_0=i)\\&=\begin{cases}p(1-p)^t & \text{if } t=nN+j-i-Z,\\0 & \text{otherwise.}\end{cases}\end{aligned} \tag{58}$$

Based on the time-enhanced characteristic matrices of the observed variable, the time-enhanced matrices of the outcomes of the D_{2i},D_{2i-1} comparison are

$$\bar{\mathbf{R}}_0(t)=\sum_{s=0}^{t}\sum_{n=0}^{\infty}\bar{\mathbf{A}}_n(s)\bar{\mathbf{A}}_n(t-s), \tag{59}$$

$$\bar{\mathbf{R}}_1(t)=\sum_{s=0}^{t}\sum_{n=0}^{\infty}\sum_{m=n+1}^{\infty}\bar{\mathbf{A}}_n(s)\bar{\mathbf{A}}_m(t-s), \tag{60}$$

$$\bar{\mathbf{R}}_{-1}(t)=\sum_{s=0}^{t}\sum_{n=1}^{\infty}\sum_{m=0}^{n-1}\bar{\mathbf{A}}_n(s)\bar{\mathbf{A}}_m(t-s), \tag{61}$$

which are given by convolution according to the time variable. For the ease of numerical analysis, we introduce the z-transformation of the characteristic matrix as $\mathbf{A}_n(z)=\sum_{t=0}^{\infty}\bar{\mathbf{A}}_n(t)z^t$, whose elements are

$$\begin{aligned}&\{\mathbf{A}_n(z)\}_{ij}=\\&=\begin{cases}pz^Z(z(1-p))^{nN+j-i-Z} & \text{if } nN+j-i-Z>0,\\0 & \text{otherwise.}\end{cases}\end{aligned} \tag{62}$$

In z-transform domain, (59)-(61) simplifies to

$$\mathbf{R}_0(z)=\sum_{n=0}^{\infty}\mathbf{A}_n(z)\mathbf{A}_n(z), \tag{63}$$

$$\mathbf{R}_1(z)=\sum_{n=0}^{\infty}\sum_{m=n+1}^{\infty}\mathbf{A}_n(z)\mathbf{A}_m(z), \tag{64}$$

$$\mathbf{R}_{-1}(z)=\sum_{n=1}^{\infty}\sum_{m=0}^{n-1}\mathbf{A}_n(z)\mathbf{A}_m(z). \tag{65}$$

Similarly to $\mathbf{A}_n$, for $n<k$, $\mathbf{A}_n(z)=\mathbf{0}$ and for $n\geq k+2$,

$$\mathbf{A}_n(z)=q(z)^{n-k-2}\mathbf{A}_{k+2}(z), \tag{66}$$

where $q(z)=(z(1-p))^N$. Using this regular structure, the $\mathbf{R}_0(z)$, $\mathbf{R}_1(z)$, $\mathbf{R}_{-1}(z)$ matrices simplify as

$$\mathbf{R}_0(z)=\mathbf{A}_k^2(z)+\mathbf{A}_{k+1}^2(z)+\frac{1}{1-q(z)^2}\mathbf{A}_{k+2}^2(z), \tag{67}$$

$$\begin{aligned}\mathbf{R}_1(z)=&\mathbf{A}_k(z)\mathbf{A}_{k+1}(z)+\frac{1}{1-q(z)}(\mathbf{A}_k(z)+\mathbf{A}_{k+1}(z))\mathbf{A}_{k+2}(z)\\&+\frac{q(z)}{(1-q(z)^2)(1-q(z))}\mathbf{A}_{k+1}^2(z),\end{aligned} \tag{68}$$

$$\begin{aligned}\mathbf{R}_{-1}(z)=&\mathbf{A}_{k+1}(z)\mathbf{A}_k(z)+\frac{1}{1-q(z)}\mathbf{A}_{k+2}(z)(\mathbf{A}_k(z)+\mathbf{A}_{k+1}(z))\\&+\frac{q(z)}{(1-q(z)^2)(1-q(z))}\mathbf{A}_{k+1}^2(z).\end{aligned} \tag{69}$$

The time during which identical D_{2i},D_{2i-1} samples are observed is characterized by the matrix

$$\hat{\mathbf{R}}(z)=\sum_{n=0}^{\infty}\mathbf{R}_0^n(z)=\left(\mathbf{I}-\mathbf{R}_0(z)\right)^{-1}. \tag{70}$$

Finally, the bit generation time is

$$T(z)=\mathbf{p}\hat{\mathbf{R}}(z)(\mathbf{R}_1(z)+\mathbf{R}_{-1}(z))\mathbb{1}, \tag{71}$$

from which the mean time to generate a bit is

$$E(\Theta)=\left.\frac{\mathrm{d}T(z)}{\mathrm{d}z}\right|_{z=1}\approx\frac{T(1)-T(1-\varepsilon)}{\varepsilon}, \tag{72}$$

which we approximate according to the rightmost expression using $T(1)=1$ and $\varepsilon=10^{-6}$.

E. The effect of dead time on the performance measures

In the deterministic grid time model, the dead time is defined as a constant $\zeta = k\tau + \delta$, where $0 \le \delta < \tau$, $k\tau$ is an integer multiple of τ which does not shift the phase of the arrival process in the τ grids, and δ represents the phase shift. Since the bit generation process depends on the difference of the consecutive D_i samples, the $k\tau$ term of the dead time does not affect many of the performance parameters, including the joint distribution of bits, the lag-r correlations and the bit generation overhead (which is measured in the number of D_i samples needed for a bit generation). It only affects the time needed to obtain a D_i sample and the bit generation time.

A similar decomposition applies for the dead time of the Erlang distributed grid model, where $Z = kN + d$, such that $0 \le d \le N-1$ and the same performance measures are insensitive to k. As a result, we restrict our attention to the case when $k = 0$ in our numerical investigations.

VIII. Numerical results

The numerical analysis results presented in this section are computed with the Erlang distributed grid time approximation, using $N = 1000$. On the one hand, increasing N above 1000 only negligibly affects the obtained results; simultaneously, the results obtained at $N = 1000$ are in good agreement with simulation results, as demonstrated below.

We used Matlab to simulate the bit generation by sampling intervals from an appropriately parametrized exponential distribution, counting them according to the continuous clock case, then generating the bits from these counts. Each presented data point is calculated from 10 million simulated intervals.

A. Joint distribution of bits

The bit generation procedure, summarized in Section II, is designed to ensure the symmetry of the generated bits, based on the assumption that $\Pr(D_1 < D_2) = \Pr(D_1 > D_2)$. Due to the consecutive D_i samples' dependence, the analysis of the bit tuple probabilities is rather complex, and we computed them based on the Erlang distributed grid time approximation.

The bit triplet probabilities as functions of the photon arrival rate–grid time product ($\lambda\tau$) are plotted in Fig. 3 using the Erlang distributed grid time analysis approach and in Fig. 4 using simulation. The product $\lambda\tau$ indicates the mean number of photon arrivals in a grid time.

Based on the coincidence of the approximate analysis and the simulation results, we consider the Erlang-based approximation with $N = 1000$ accurate enough and present only the Erlang-based approximate analysis results in the rest of the section despite the availability of similarly accurate simulation results.

The results in Figs. 3 and 4 verify the consequence of Corollary 2 and the law of total probability (as it is detailed right after Theorem 2) that the bit triplet probabilities—also with non-zero dead time—depend on the number of $0 \to 1$ or $1 \to 0$ *transitions* and the same probabilities are observed

- for 000 and 111 with no *transition*,
- for 001, 011, 100 and 110 with one *transition*,
- for 010 and 101 with two *transitions*.

The bit 4-tuple probabilities are depicted in Fig. 5 with 4 different dead times. Theorem 4 applies for zero dead time ($\delta/\tau = d/N = 0$); consequently, there are 4 different probabilities. Theorem 4 does not apply for the other 3 cases ($\delta/\tau = d/N = 0.3, 0.5, 0.9$), but Corollary 2 does, and this way the number of different probabilities is less than 2^4, but more than 4 in the related plots. For $\delta/\tau = 0.3$, the plot indicates 4 different curves from $\lambda\tau = 0$ to ~ 4.5, two curves fork at around $\lambda\tau \sim 4.5$ and composes 6 curves from $\lambda\tau \sim 4.5$ to 10. A similar tendency appears at $\delta/\tau = 0.5$, but in this case, the curves fork at around $\lambda\tau \sim 2$. To indicate the relation of the probability ranges with different dead times, the scaling of the y-axis is the same in each figure.

The plots also indicate a kind of cyclic behavior as a function of the dead time. Starting from a regular deviation at $\delta/\tau = 0.1$ in Fig. 3 and $\delta/\tau = 0$ in Fig. 5, the plots highly deviate at around $\delta/\tau = 0.5$ and get close to the regular deviation (similar to the one at $\delta/\tau = 0, 0.1$) at $\delta/\tau = 0.9$.

Similar behavior can be observed in the bit 5-tuple probabilities in Fig. 6. For zero dead time ($\delta/\tau = 0$), Theorem 4 ensures 5 different curves at most, and for non-zero dead time ($\delta/\tau = 0.5$), we have more than 5 different probabilities.

To summarize, we have not found a simple, intuitive explanation for the particular behavior of the curves in Figs. 3–6. We only recognize that the bit n-tuple probabilities significantly deviate from the uniform value, 2^{-n}, at high photon arrival rates when the dead time is around $\delta/\tau \sim 0.5$; and the bit n-tuple probabilities converge to the uniform value as the photon arrival rate tends to zero independent of the dead time. The latter observation is natural since the dependence of the D_i values on the phase of the photon arrival vanishes when the photon arrival rate is low and the mean photon interarrival time ($1/\lambda$) is much larger than the grid time τ.

B. Lag-r correlations

The joint distribution of bit n-tuples carries the most detailed information on the bit generation process, and many further performance measures can be derived based on that. The lag-1 and lag-2 correlations are depicted in Fig. 7.

In agreement with the bit triplet probability results, the lag-r correlations vary significantly for high photon arrival rates, and the dead time, δ/τ, significantly affects the behavior. While finding an interpretation for the particular curves is difficult, the relation of the lag-r correlations and the bit triplet probabilities are readable from the figures.

In the case of $\delta/\tau = 0.1$, the lag-1 correlation is significantly positive from $\lambda\tau = 1$ to 6 and decays to zero for larger $\lambda\tau$ values, while the lag-2 correlation is negligible along the whole plotted range. It agrees with the bit triplet probabilities in Figs. 3 and 4, where the triplets with identical bits, 000 and 111, have a higher probability than the uniform value between $\lambda\tau = 1$ to 6. They converge to the uniform value for higher $\lambda\tau$. At the same time, the triplets with 2 *transitions*, 010, and 101 have lower probabilities than the uniform one. For $\delta/\tau = 0.9$, the lag-1 correlation is significantly positive. The lag-2 correlation is negligible in the whole plotted range, and the triplets with identical bits have a higher probability than the uniform in the whole range.

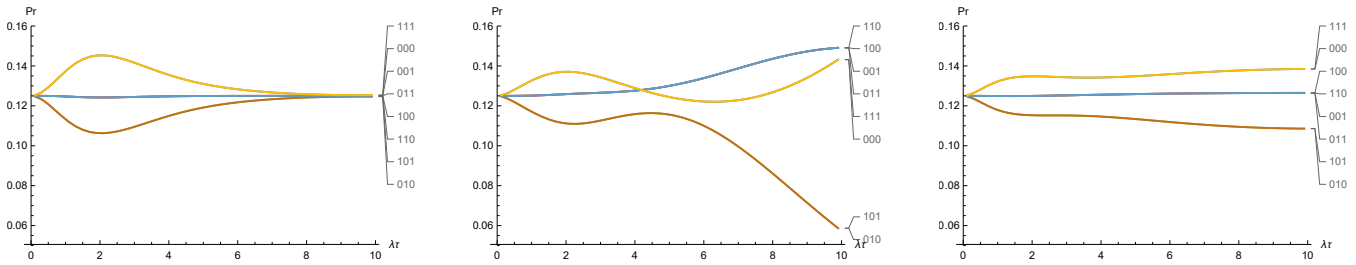

Figure 3. Probabilities of bit triplets with $\delta/\tau = 0.1, 0.5, 0.9$ computed by the Erlang distributed grid approximation

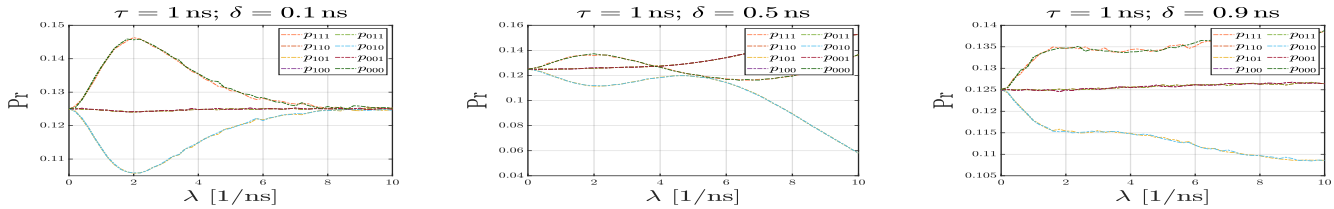

Figure 4. Simulated probabilities of bit triplets with $\delta/\tau = 0.1, 0.5, 0.9$

The case of $\delta/\tau = 0.5$ is rather interesting at around $\lambda\tau = 5$, where the lag-1 correlation is close to zero, and the role of the lag-2 correlation becomes dominant. At this point, the lag-2 correlation is significantly negative, which means that the bit triplets, whose first and last bits are different—001, 011, 100, and 110—are more probable, as it is in Figs. 3 and 4. At higher $\lambda\tau$ values, the lag-1 correlation increases, but the lag-2 correlation decreases significantly, and the bit triplets with different first and last bits remain more probable than the uniform probability.

In all cases, the lag-r correlation converges to zero as the photon arrival rate tends to zero, which aligns with the convergence of the bit triplet probabilities to the uniform value as the photon arrival rate tends to zero.

C. Bit generation overhead and bit generation time

The mean bit generation overhead and the mean bit generation time, defined in (57) and (72), are provided in Fig. 8. The minimum number of D_i samples needed to generate a bit is 2, and it is obtained when $D_{2i} \neq D_{2i-1}$. As expected, the mean of ρ is always above 2. With increasing photon generation rate, $E(\rho)$ gets to be strongly dependent on δ/τ in a somewhat symmetric way. When $\delta/\tau \approx 0.5$, $E(\rho)$ decays toward 2 with increasing photon generation rate, while when $\min\{\delta/\tau, (\tau-\delta)/\tau\} \approx 0$, $E(\rho)$ increases with increasing photon generation rate.

An intuitive reason for this behavior is as follows. If $\min\{\delta, \tau-\delta\} \approx 0$, say $\delta/\tau = 0.1$ and $\lambda\tau \gg 1$, say $\lambda\tau = 10$, then 5 observed photon arrivals occur in a τ long interval on average—$5(\delta + 1/\lambda)/\tau = 1$)—, that is, in a typical experiment according to the average behavior, 4 consecutive D_i samples equal 0 and the next one equals 1. The 4 consecutive identical D_i samples are dropped, which makes $E(\rho)$ high. We note that the case of $\delta/\tau = 0.9$ and $\lambda\tau = 10$ is even more inefficient. In this case, the average behavior is such that the arrivals always occur in the same phase, since after an arrival, further photon arrivals are blocked for $\delta/\tau = 0.9$. After the dead time, the average time of the subsequent photon arrival is $1/\lambda = 0.1\tau$. If the first arrival occurs in $(0, 0.9\tau)$ then, according to the average behavior, all $D_i = 0$, and in the opposite case, if the first arrival occurs in $(0.9\tau, \tau)$, then all $D_i = 1$. In either case, the consecutive D_i samples are dropped because they are identical.

As $\lambda\tau$ tends to zero, the D_i samples get large, and the probability that the consecutive D_i samples are identical decreases to zero. This way, all D_i sample pairs generate a bit, and ρ tends to 2.

The ideal behavior is obtained in all evaluated performance measures as the photon arrival rate tends to zero. In that case, the bit triplet probabilities converge to the uniform value, the correlation tends to zero, and the bit generation overhead reaches its minimum, $\rho = 2$. The real cost of reducing the photon arrival rate towards zero is indicated in the right plot of Fig. 8. The time of a bit generation increases with the inverse of the photon arrival rate. When $\lambda\tau$ is close to zero, $E(D_i) \approx 1/(\lambda\tau)$, the probability of identical consecutive D_i samples tends to zero, and this way, the mean bit generation time tends to $2/\lambda$.

IX. Conclusion

We have considered the QRNG procedure described in Ref. [1], and introduced analysis approaches to quantify the properties of the generated random bits. To the best of the authors' knowledge, the inverse-reverse relation provided in Theorem 2, the mathematical analysis of the joint distribution and correlation of the generated random bits were not available before. The exact analysis approach, based on the deterministic grid time assumption, indicates the correlation of the consecutive bits with the help of a characteristic function. However, it

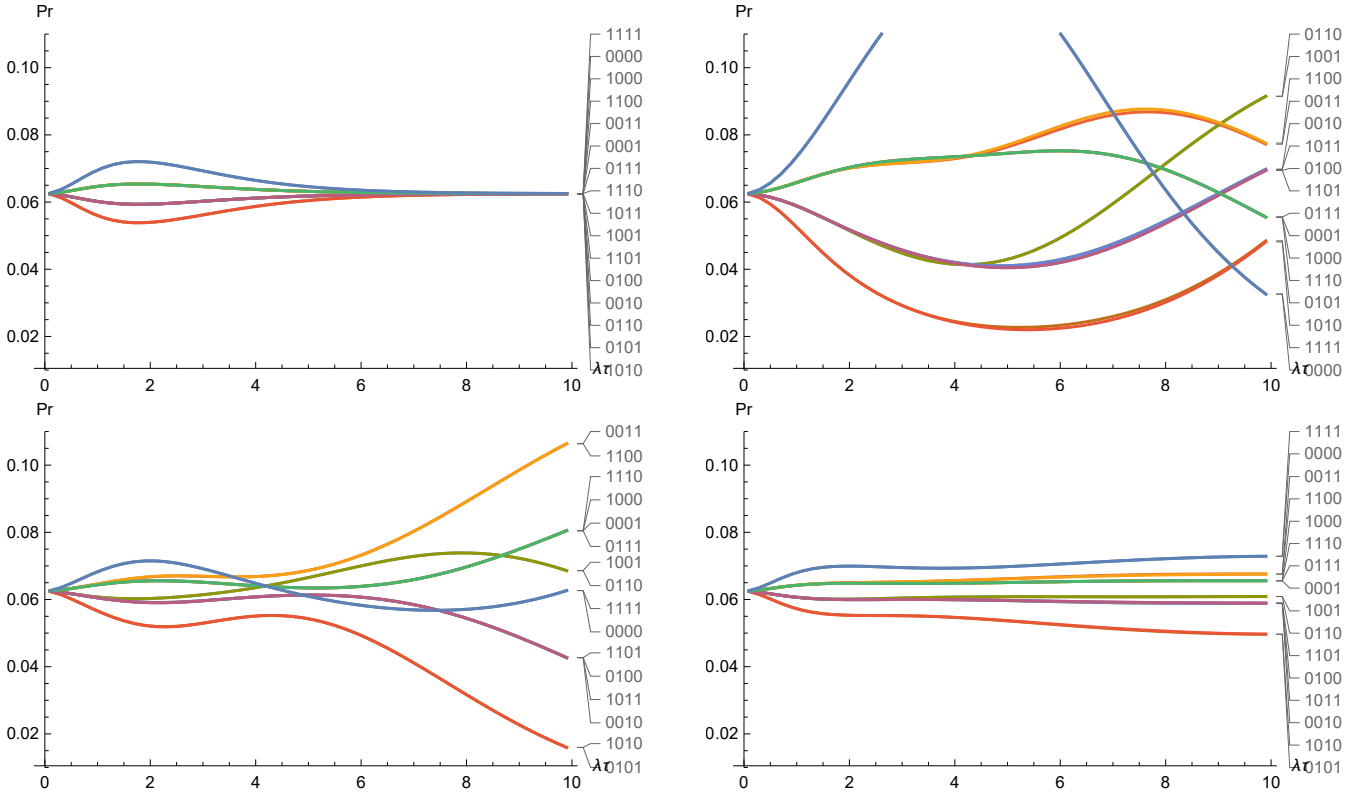

Figure 5. Bit 4-tuple probabilities with $\delta/\tau = 0, 0.3, 0.5, 0.9$ (upper-left, upper-right, lower-left, lower-right, respectively) as a function of the normalized photon arrival rate $\lambda\tau$

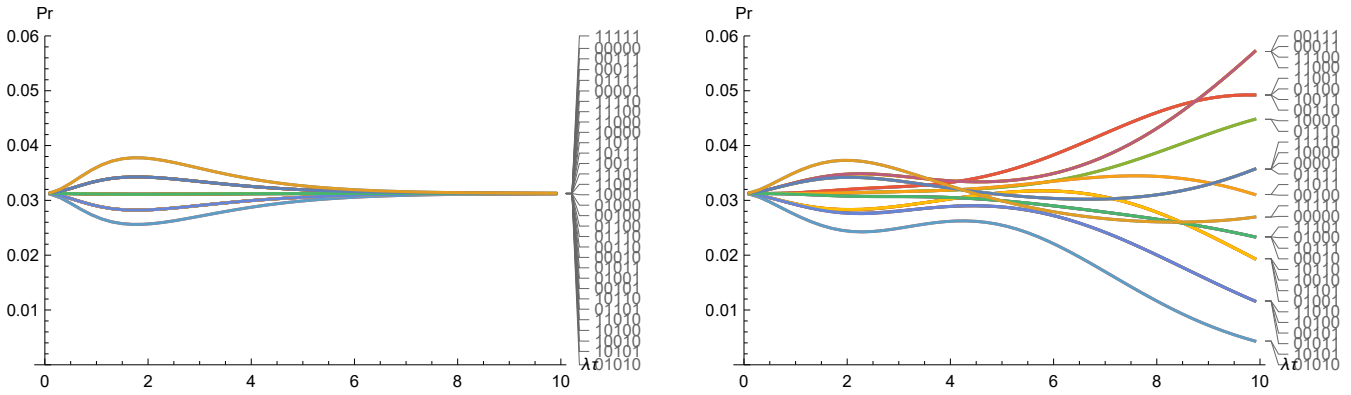

Figure 6. Bit 5-tuple probabilities with $\delta/\tau = 0, 0.5$ as a function of the normalized photon arrival rate $\lambda\tau$

gets inhibitively complex to compute the performance measures of interest.

To overcome this limitation, we introduced an approximate analysis approach based on the Erlang distributed approximation of the deterministic grid time. This approach allows the computation of the performance measures of interest, and its accuracy is verified against simulation. In future work, we intend to extend the introduced analysis approach to different bit generation methods based on the same physical process.

Acknowledgment

The authors are thankful for the fruitful discussions and the advises of Illés Horváth (ELKH-BME Information Systems Research Group, Budapest, Hungary). M. Telek was supported by the OTKA K-138208 project of the Hungarian Scientific Research Fund. B. Solymos and Á. Schranz were supported by the Ministry of Culture and Innovation and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1-NL-2022-00004). Á. Schranz was also supported by the OTKA K-142845 project of the Hungarian Scientific Research Fund.

References

[1] M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Review of scientific instruments*, vol. 78, no. 4, p. 045104, 2007.

[2] M. Herrero-Collantes and J. C. García-Escartín, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

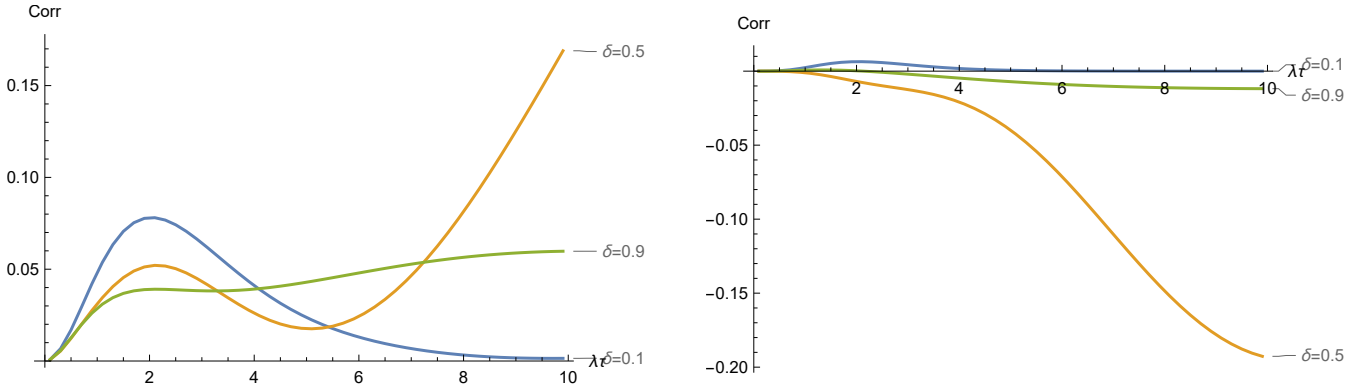

Figure 7. Lag-1 and lag-2 correlation as a function of the normalized photon arrival rate with different dead times.

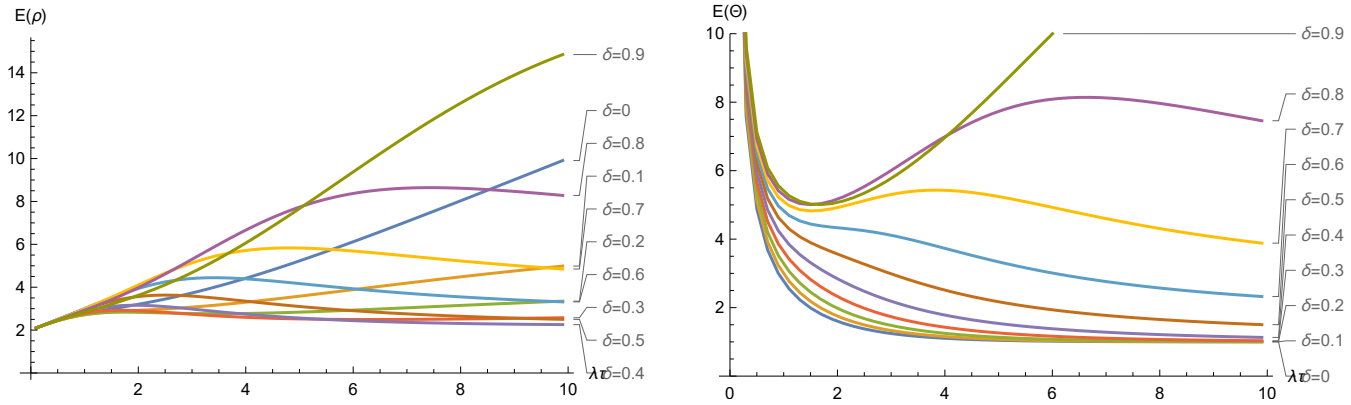

Figure 8. Mean bit generation overhead, $E(\rho)$, and mean bit generation time, $E(\Theta)$, as a function of the normalized photon arrival rate with different dead times.

[3] L. Gyöngyösi, L. Bacsardi, and S. Imre, "A survey on quantum key distribution," *Infocommunications Journal*, vol. 11, no. 2, pp. 14–21, 2019.

[4] H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," *Applied optics*, vol. 44, no. 36, pp. 7760–7763, 2005.

[5] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Applied physics letters*, vol. 93, no. 3, p. 031109, 2008.

[6] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *Journal of Modern Optics*, vol. 56, no. 4, pp. 516–522, 2009.

[7] L. Yu, M. Yang, P. Wang, and S. Kawata, "Note: A sampling method for quantum random bit generation," *Review of Scientific Instruments*, vol. 81, no. 4, p. 046107, 2010.

[8] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Applied Physics Letters*, vol. 98, no. 17, p. 171105, 2011.

[9] K. Kravtsov, I. Radchenko, S. Kulik, and S. Molotkov, "Minimalist design of a robust real-time quantum random number generator," *JOSA B*, vol. 32, no. 8, pp. 1743–1747, 2015.

[10] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermann, "A monolithic silicon quantum random number generator based on measurement of photon detection time," *IEEE Photonics Journal*, vol. 7, no. 5, pp. 1–13, 2015.

[11] R. S. Hasan, S. K. Tawfeeq, N. Q. Mohammed, and A. I. Khaleel, "A true random number generator based on the photon arrival time registered in a coincidence window between two single-photon counting modules," *Chinese journal of physics*, vol. 56, no. 1, pp. 385–391, 2018.

[12] A. Tomasi, A. Meneghetti, N. Massari, L. Gasparini, D. Rucatti, and H. Xu, "Model, validation, and characterization of a robust quantum random number generator based on photon arrival time comparison," *Journal of Lightwave Technology*, vol. 36, no. 18, pp. 3843–3854, 2018.

[13] H. Xu, N. Massari, L. Gasparini, A. Meneghetti, and A. Tomasi, "A spad-based random number generator pixel based on the arrival time of photons," *Integration*, vol. 64, pp. 22–28, 2019.

[14] N. Massari, L. Gasparini, M. Perenzoni, G. Pucker, A. Tomasi, Z. Bisadi, A. Meneghetti, and L. Pavesi, "A compact tdc-based quantum random number generator," in *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*. IEEE, 2019, pp. 815–818.

[15] A. Stanco, D. G. Marangon, G. Vallone, S. Burri, E. Charbon, and P. Villoresi, "Certification of the efficient random number generation technique based on single-photon detector arrays and time-to-digital converters," *IET Quantum Communication*, vol. 2, no. 3, pp. 74–79, 2021.

[16] A. Schranz and E. Udvary, "Mathematical analysis of a quantum random number generator based on the time difference between photon detections," *Optical Engineering*, vol. 59, no. 4, p. 044104, 2020. [Online]. Available: https://doi.org/10.1117/1.OE.59.4.044104

[17] V. Ramaswami, D. G. Woolford, and D. A. Stanford, "The Erlangization method for Markovian fluid flows," *Annals of Operations Research*, vol. 160, no. 1, pp. 215–225, 2008.

[18] M. Telek, "Transient analysis of Markov modulated processes with Erlangization, ME-fication and inverse Laplace transformation," *Stochastic Models*, vol. 38, no. 4, pp. 638–664, 2022.