



5-bit all-optical quantum random number generator based on a time-multiplexed optical parametric oscillator

SHAOJIE LI,¹ XIAOXUAN ZHU,¹ JINTAO FAN,^{1,3} KAI WEN,² AND MINGLIE HU^{1,4} 

¹Ultrafast Laser Laboratory, Key Laboratory of Opto-electronic Information Science and Technology of Ministry of Education, School of Precision Instruments and Opto-electronics Engineering, Tianjin University, 300072 Tianjin, China

²Beijing QBoson Quantum Technology Co., Ltd., Beijing 100015, China

³fanjintao@tju.edu.cn

⁴huminglie@tju.edu.cn

Abstract: Random numbers are of critical importance in many applications, including secure communication, photonics computing and cryptography. Due to the non-deterministic nature of the quantum processes, a degenerate optical parametric oscillator (DOPO) constitutes a solution to produce true randomness. Nevertheless, one of the existing challenges for DOPO in this field is bit sequence scalability. Here, we experimentally report on the generation of 5-bit random number streams in a time-multiplexed femtosecond DOPO system. A multi-pass cell is added to elongate the OPO cavity to scale up the bit sequences. To this end, for a ~ 15 m long all free space OPO cavity, resonating 5 signal pulses with a repetition rate of 50 MHz is demonstrated. The above-threshold binary phase nature originates from vacuum fluctuations of a DOPO ensuring the randomness of the system. The phase state of the output is characterized by the interference pattern between the output pulses and the fundamental pump pulses. Different bit sequences are presented here by turning on and off the OPO. Conditional probability is performed to verify the randomness of the output for 1200 bits. Our scheme provides a new direction for an all-optical random number generator.

© 2023 Optica Publishing Group under the terms of the [Optica Open Access Publishing Agreement](#)

1. Introduction

Random numbers are a critical ingredient in diverse applications, including gaming, sampling, scientific simulations and cryptography [1,2]. In fact, it's incredibly challenging for humans to create an arbitrarily long and random string of numbers. Consequently, researchers have long searched for the ideal source of random numbers. Random number generators (RNGs) are hardware devices or software algorithms that produce random numbers from a limited or unlimited distribution. There are mainly two types of RNGs: pseudorandom number generators (PRNGs) and true (physical) random number generators (TRNGs). Among them, PRNGs depend on a computational algorithm for outputting a sequence of numbers whose properties approximate true randomness. They have the advantages of being fast and easy to create, and thus could be used in computer languages like Python and applications such as key stream generation. However, given that algorithms are commonly based on distributions, random numbers generated in this way are not truly random, and hence not secure enough. If the seed and algorithm are known, the numbers generated are deterministic and predictable. As a result, PRNGs are not suitable for cryptographic implementations with high security requirements. Another type of RNGs, TRNGs, depending on an external unpredictable physical variable, i.e., entropy, the decay time of radioactive material, thermal noise of semiconductor devices, are more secure since they exhibit truly and completely random behavior. Therefore, TRNGs play an important role in

cryptographic keys, signature parameters and so on. Owing to the fact a TRNG is based on physical processes, it considers physical attributes of the system and also measurement biases. However, TRNGs often rely on deterministic post-processing algorithms to further improve randomness. Consequently, despite the availability of physical processes, delivering genuine random numbers is a matter of great concern and an ongoing subject.

For provably secure random number generation, quantum-mechanical systems that produce the ultimate in randomness provide a nearly ideal answer. Due to the non-deterministic fundamental unpredictable nature of quantum effects, quantum random number generators (QRNGs) stand out as the new standard of random number generators. Over the past few decades, various types of QRNGs have been designed and proposed, including time of arrival generators [3–6], Raman scattering (Interaction with phonon fluctuations) [7,8], measuring amplified spontaneous emission (ASE) [9–11], homodyne measurement of the vacuum fluctuations [12–14] and photon counting [15,16]. Nevertheless, in most of these QRNG schemes, the tedious post-processing work complicates the actual system, which poses great challenges to practical applications. To give a simple example, in a vacuum fluctuations [12–14] detection scheme, photodetection is an essential part. However, the security of the original data will be affected by the electrical noise of the experiment device. Therefore, choosing a random number extraction method to eliminate classical noise and ensure the purity of the state is the top priority. This inspires us to propose a QRNG system independent of postprocessing scheme.

Over the past few years, degenerate optical parametric oscillator (DOPO) give rise to a diversity of interesting nonlinear dynamical behaviors such as temporal solitons, phase transitions, and dissipative quadratic solitons [17–19]. From the application point, DOPOs based on second order nonlinearity process have been proven to be an ingenious all-optical way for true random number generation and coherent Ising machine [20,21]. In principle, DOPOs have proven to be a physical system that undergoes a second-order phase transition [18]. Below threshold, the signal field represents a vacuum state, also referred as stochastic vacuum fluctuations. When increasing pump above threshold, this unstable state will decay into one of two degenerate energy minima with equal probability, where the corresponding two-phase states, $\{0\}$ or $\{\pi\}$ related to the fundamental pump. In other words, the DOPO's output phase exhibits a two-state output above threshold, which can be interpreted as a binary bit, or the head and tail of a coin toss. In 2012, Marandi et al. utilize such bi-phase state generation in a pulsed degenerate OPO to realize an all-optical RNG [21]. Note that, in this case, classical noise effects can be negligible and electronic or computer post-processing can be minimized, which greatly reduced the complexity of the system and protect the randomness nature. In consequence, the DOPO works well as a PRNG just like a fair coin tossing, the binary phase amplified from vacuum noise leads to unbiased two bit number output. Recently, Tobias et al. demonstrated another type of all optical QRNG by implementing a nondegenerate OPO operated in the period-doubling region [22]. Under this condition, there are only two possible output states that can be regarded as 0 and 1 without any ambiguity. The output states are totally determined by the randomness of the quantum vacuum fluctuations in the optical cavity, and hence the generated bit number is random with perfect entropy. We note that for practical applications, bit strings scalability is of fundamental importance, however, in two recent QRNGs, the number of the bit spins is limited to be one. In other words, only "0" or "1" can be obtained (equally to only a single optical coin is tossed) when the system is pumped well over threshold and allowed to reach steady state, which is constrained by either complexity to implement or difficulty to control the physical dynamics in the cavity.

In this paper, we show that the insertion of a multi-pass cell (MPC) in a DOPO cavity leads to a time-division-multiplexed DOPO, which enables 5-bit strings random number generation. Beneficial from the MPC scheme, in terms of the 50 MHz repetition rate of the pump laser, the DOPO pulses resonated in a ~ 15 m equivalent linear cavity in a compact design. In the proposed system, five temporally multiplexed OPO pulses locate in one of two possible phase states marked

as bit value 0 or 1 when increasing the pump power above the threshold. The bit stream of the outcome is performed by interfering the DOPO pulses with the fundamental pump pulses, no additional bit extraction is demanded. Since the binary phase is born in the nonlinear crystal as vacuum fluctuations, the output presents unpredictability, resulting in a well-balanced coin toss result. This has been further confirmed by analyzing the distributions of 1200 bits measurements. Thanks to its all-optical nature, our system has the capability of realizing high speed, energy- and bit value-scalable random number generation.

2. Principle and experimental setup

In a DOPO, the system is always driven by a synchronous pulsed pump whose central frequency is marked as $2\omega_0$ (second harmonics of the fundamental pump centered at frequency ω_0), while the resonant signal and idler are centered at half-harmonic frequency ω_0 . As can be seen that the signal and idler pulses share the same frequency, pulse envelope and polarization, such a strong coupled nature could give birth to rich nonlinear dynamics around degeneracy. An excellent example is spectral phase transition below and above the oscillation threshold. The signals experience a totally squeezed vacuum state below the threshold; however, when the pump power is increased above the threshold, the signal will unpredictably choose one of two possible phase states, 0 or π phase relative to the fundamental pump phase. The generated state can be marked as a binary bit 0 and 1. Since the binary phase is inherited from vacuum noise, the resulting phase is equally likely to position at 0 and π , and thus, DOPO can be regarded as a perfect optical coin toss. The length of the bit sequence is determined by the number of DOPOs.

Guided by the above principle, to further avoid implementing N matched resonators, we propose our 5 DOPO system by introducing an MPC in a time-division multiplexed DOPO. Figure 1(a) illustrates the schematic of the designed system. The used fundamental pump source is a commercially available 50 MHz, 1030 nm Yb fiber laser system (BFL-1030-10LEW) with an output power of 12.5 W and pulse duration of 247 fs. The output pulses are firstly launched into a 2.4 mm LiB_3O_5 (LBO) crystal, where a green pulse train centered at 515 nm is generated via second harmonic generation process. Up to 4.8 W of the average power of green light has been achieved. A dichroic mirror is used to separate the undepleted pump. The green light is then injected into the DOPO parametric gain medium through a concave silver coated mirror (M1, radius of curvature: 200 mm). The pump beam has a waist diameter of $23.6\ \mu\text{m}$ at the center of the gain crystal. A 3 mm long beta barium borate (BBO) crystal with $\theta = 23.3^\circ$ is selected as gain medium to provide degenerate parametric gain for a pump centered at 515 nm with type I phase matching. After the parametric process, the outcome light is collimated with another silver-coated mirror (M2). The other mirrors in the cavity are all dielectric mirrors with the same coating, which is highly transmissive at the pump wavelength and highly reflective from 650 to 1100 nm. The signal pulses are extracted with an output coupling mirror (OC) with a 5% output ratio.

Apart from this, an MPC unit is inserted in the DOPO cavity, which is an essential part of our system. The MPC scheme is commonly implemented in Herriott-type, composed of two concave mirrors, for post compression of ultrashort pulses. As point out in [23], MPCs have the advantages of excellent beam quality and low loss under simple and economic conditions. Herein, the MPC is adopted to elongate the OPO cavity. The bounce number on the mirrors and the separation of the MPC are recorded as 13 times and 80 cm, respectively. In this manner, the optical path length of the linear DOPO cavity is $\text{LOPO} = 15\ \text{m}$, which is 5 times that of the pump oscillator cavity. Given the linear cavity type, the corresponding roundtrip time in DOPO is calculated to be $\sim 100\ \text{ns}$, while the pump laser has a roundtrip time $\sim 20\ \text{ns}$. Obviously, the cavity can accommodate 5 DOPO pulses. As shown in Fig. 1(b), in every 5 pulses, the signal pulse interacts directly with a pump pulse and experiences gain, but the next 4 pump pulse repetition period only propagates in the DOPO cavity. Since the DOPO pulses all grow from a vacuum

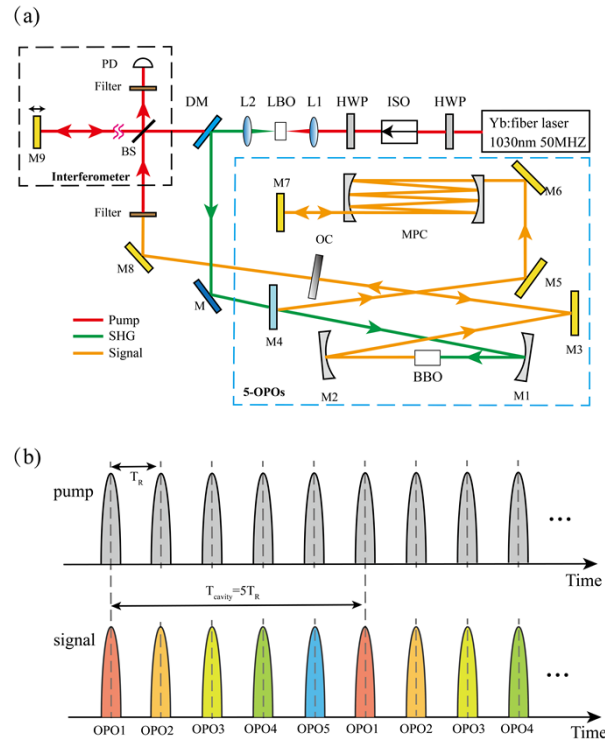


Fig. 1. (a) Experimental setup of the proposed QRNG. The DOPO includes 5 signal pulses circulating in the cavity. A Michelson interferometer is used to measure the relative phase states of the DOPO output pulses and fundamental pump pulses. DM: dichroic mirror (HR 515, AR 1030), HWP: half-wave plate, M: mirror, MPC: multi-pass cell, OC: output coupler, BS: beam splitter, PD: photodetector, (b) Illustrations of pulse trains of the pump and DOPO, where the OPO cavity roundtrip time is 5 times that of the pump oscillator cavity.

noise, the 5 pulses circulating in the cavity are indistinguishable, showing the same polarization, spectrum and pulse width except the phase state. Thus, 5 independent DOPO pulses with random uniformly distributed selection phase states are well prepared.

To measure the phase state of DOPOs, the signal pulses and undepleted pump pulses are sent to a Michelson-like interferometer, as shown in the dashed square in Fig. 1(a). A 3 nm bandwidth narrow bandpass spectral filter is introduced in the photodiode path to increase the interference contrast. Then, by fine adjusting the temporal delay in between, the interference pattern is detected by a photodiode and recorded by a 5-GHz oscilloscope (Rigol Oscilloscope, DS70504, 5 GHz, 4 Channel, 20 GS/s).

3. Results and discussions

First, we illustrate a typical behavior of the DOPO depending on the cavity length tuning. The OPO is pumped with the maximum average output power of the SHG green light. To observe the oscillation, we slowly varied the cavity length through M7, which is mounted on a linear translation stage. As shown in Fig. 2, both degenerate oscillations and far-from-degenerate oscillations can be achieved during this process. We notice that the oscillation only occurs in some discriminative points, similar with demonstrations in [24]. This can be attributed to the phase relation shape between the pump and output pulses. In the degenerate case, as shown at the bottom of the Fig. 2, the signal and idler are indistinguishable, the spectrum is centered at

1034 nm. While in the non-degenerate case, the signal and idler are separated, as depicted in Fig. 2(a)-(c). In Fig. 2(d), the oscillator state in between degenerate and non-degenerated point can be called nearly degenerate. As can be seen, the power in the longer wavelength part is lower than that of the shorter wavelength range. This is influenced by the coating range of the mirrors, the longer wavelength part is close to the edges of the mirror bandwidth. Moreover, the spectra bandwidth towards the longer wavelength is increased. This can be ascribed to the accumulated intracavity third order dispersion, resulting in lower chirp at longer wavelength.

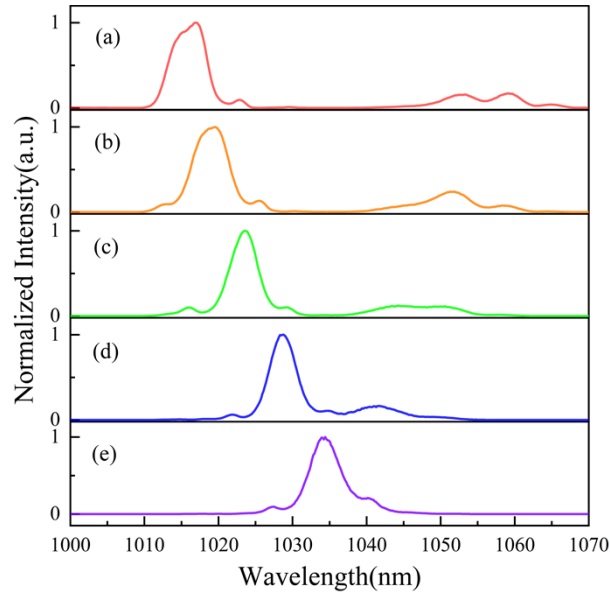


Fig. 2. The state of OPO output light at degenerate point and non-degenerate point varies with the length of the cavity. (a)-(c) show the non-degenerate spectra; (d) show the nearly degenerate state; (e) output spectrum of DOPO at degeneracy.

Then, we show the stability of the OPO system, no stabilization on the pump and cavity is performed. Below a pump power of 2.96 W, no signal pulses occur except for vacuum fluctuations. That is to say, the threshold green pump power is marked to be 2.96 W. This is reasonable considering the coating losses of the BBO crystal, mirrors and also the MPCs. By further increasing the pump power, the output power of the DOPO rises. When the OPO is pumped with 4 W, the signal of the DOPO has 50 mW of average output power at degeneracy with the spectrum shown in Fig. 3(b) (blue line). For comparison, the red line here presents the spectrum of the fundamental pump. Except for some small modulations in the output spectrum, these two curves show a good agreement. We attribute these modulations to the group delay dispersion of the whole cavity elements. In Fig. 3(a), the power evolution at degeneracy point is recorded. It can be found that the output power varies 50 mW over 10 mins, the corresponding RMS noise is calculated to be 3.5% RMS. The RMS measured here is larger than that of the pump laser. The variation of power is related to air fluctuation, temperature change, mechanical vibration and some others. To suppress the long-term instability caused by the environmental disturbance, we can isolate the system in a closed box. In addition, one can actively stabilize the DROPO at the degeneracy by using a phase locked loop circuit based on dither or dither free locking scheme [25]. Actually, in most quantum computation or entropy cases, the calculation should be completed in milliseconds, thus the stability requirement of system has been already achieved.

Next, we perform a measurement to examine the effectiveness of the proposed QRNG by recording temporal interference signal between the DOPO output pulses and the undepleted

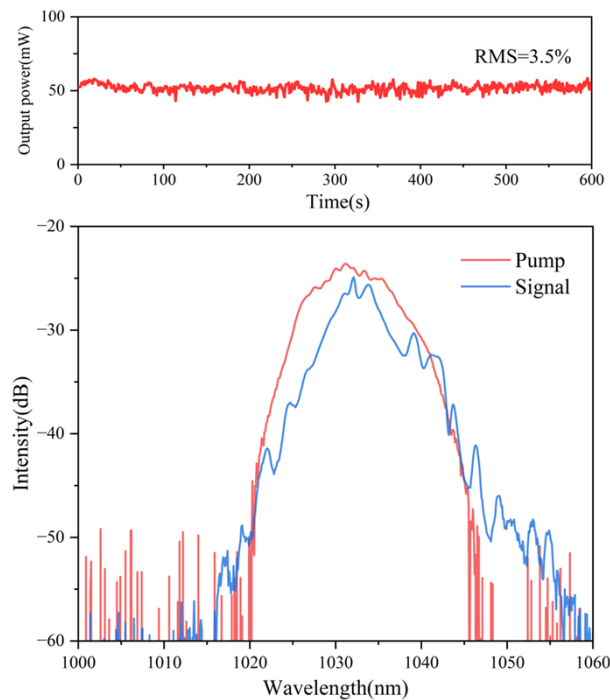


Fig. 3. (a) Power stability test of DOPO output. The red lines represent the average power over 10 mins. (b) Spectrum of the output signal (blue line) and the fundamental pump (red line).

pump. Due to the binary phase distribution of DOPO, the output phase is taken as 0 or π relative to the fundamental pump, thus, constructive and destructive interference patterns are observed, respectively. By simply defining a threshold, constructive interferences lead to high-intensity interferometer outputs, associated with a result of 1, while destructive interference results in a low-intensity interferometer output, assigned a value of 0. For different random number sequences generation, the OPO is turned on and off by a chopper. Figure 4 shows the results of a random number sequence at a chopper frequency of 2 kHz, the chopper used here is to suppress and restart the DOPO oscillation, since the binary phase state stems from vacuum noise, when the DOPO restarts, there is a 50% chance of the output binary value being distributed as 0 or 1. As can be seen from Fig. 4, the variation of the output power doesn't affect the quality of the generated bit numbers when we maintain the pump power well above pump threshold. Only when we force the pump power below the pump threshold, the signal needs to grow up through vacuum noise, in this case the output phase states will change. As shown in the inset of Fig. 4, the bit sequence changes from "10000" to "01110" when the DOPO system restarted.

As expected, by assigning binary values to the relative phase states of the DOPO outputs, our results are associated with a series of 5-bit random numbers. Here, we turn on and turn off the DOPO system periodically at a clock rate of 10 kbps. Figure 5(a)-(f) shows six different sequences of the generating 5-bit streams in the generator. The red and blue areas denote the two possible phase states 1 and 0. In this way, the results of Fig. 5(a)-(f) are read as 00111, 01000, 11000, 11001, 10101, and 10001, respectively. Intuitively, only two intensity levels exist, no other intensity level occurs. This further indicates that only two distinct phase states are excited in the DOPO cavity. In addition, the measured alternative bit streams also confirm the robustness of the system, which could eliminate the influences of air fluctuations, thermal effects, and also

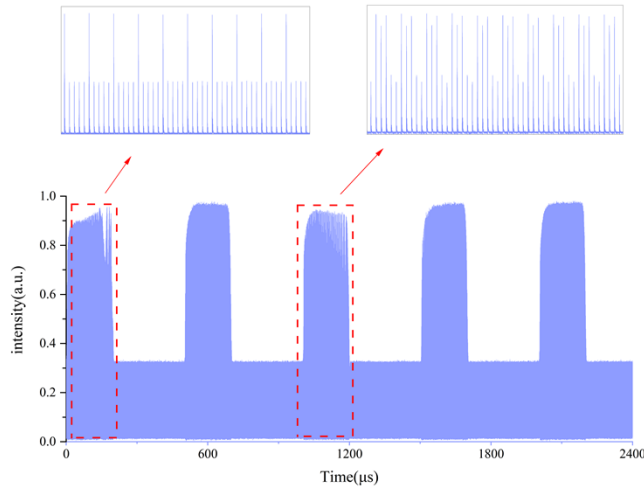


Fig. 4. A random number sequence measured at a chopper frequency of 2 kHz

pump intensity fluctuations. Otherwise, the randomness of the output will be disturbed and the interference pattern will exist at other unwanted intensity levels except for the measured two. We stress that as many as 32 different 5-bit sequences could be excited in the proposed system. The results observed above present the perfect unbiased randomness of our generator, which indicates the quantum effects occurring in DOPO make it an excellent source of QRNG.

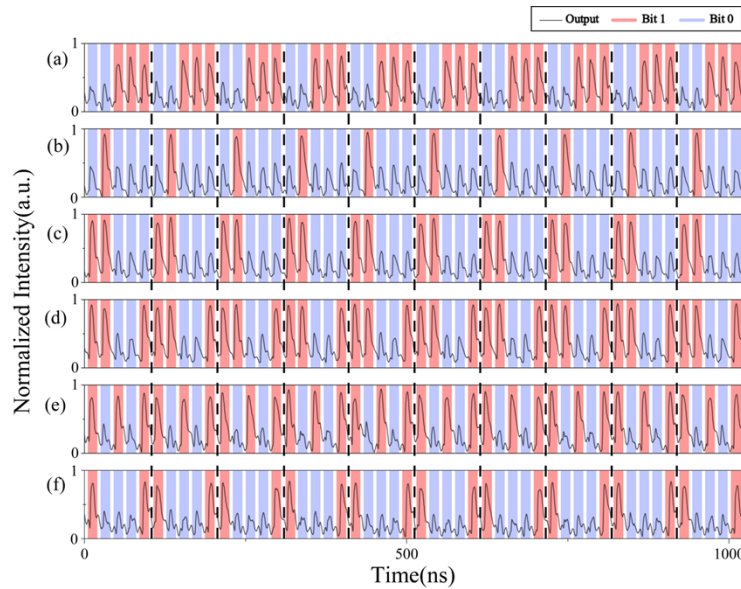


Fig. 5. The time domain measurements of all optical RNG based on degenerate OPO. (a)-(f) represent different output results in the DOPO through turn-“on” and turn-“off” the system accompanied by a 10 kbps clock signal. ‘0’ and ‘1’ correspond to the intensity of the interference.

Finally, we evaluate the pure randomness of the output of our all-optical QRNG by collecting up to 240 groups of 5-bit sequences, which corresponds to 1200-bit numbers. While the Alphabet,

NIST Statistical Test Suite, and Dieharder are widely used to examine the randomness of the bit sequence, a complete test needs a very large number of data and takes hours. Confined by the storage capability of the oscilloscope, we use an alternative way named as conditional probability to evaluate the quality of the DOPO outputs. As explained in [26], the objective conditional probabilities which are independent of the underlying state and stem from a certain purely algebraic relation between the events, and an axiomatic approach to quantum mechanics. As a result, the conditional probability could indicate the randomness of our QRNG. We calculate the probability of both the bit value distribution and the conditional probability of the bit streams. It can be seen from Fig. 6 that the probabilities of values 1 and 0 are both close to $1/2$ (49.9% for 0, and 50.1% for 1), which indicates that the DOPO output phase satisfies the basic level of statistical randomness. The conditional probability, defined as $p(x|y) = p(x \wedge y)/p(y)$, represents whether the subsequent result is affected by the previous oscillation state. As a simple example, $p(0|1)$ denotes the probability of getting a result of 0 after the previous result was 1. Ideally, when the two events are independent, the conditional probability should be $1/2$. Obviously, all the data shown in Fig. 6 are equally probable (close to $1/2$), which means that there is no particular preference for subsequent outputs. The analysis above shows that the neighboring bit is independent, and hence there is no memory storage in the DOPO phase output. The small bias may come from the limited bit streams. The balance of two probabilities and the independence of adjacent bit outcomes implies that the proposed system could serve as an all-optical randomness generator.

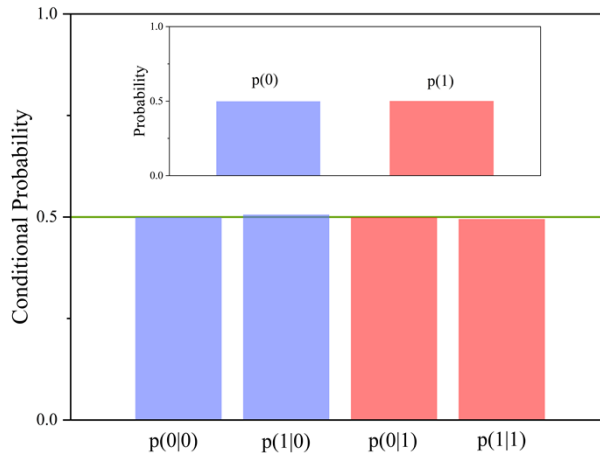


Fig. 6. The conditional probabilities of different options for the result of QRNG. The sample size is 1200 bits and the green line represents the conditional probability value in the ideal case. Insert: The probability of bit value of 0 and 1 in the sequences indicated by the blue and red areas, respectively.

4. Conclusion

In summary, we have proposed a 5-bit all-optical QRNG based on a time-multiplexed degenerate OPO. With the help of the MPC unit, OPO can accommodate five signal pulses. The randomness is attributed to the quantum effect of DOPO, random number generation is realized by measuring the interference between signal and pump with a photodetector, which does not require a lot of post-processing and simplifies the complexity of the system. Up to 50 mW output power is obtained with 3.4% RMS. Both bit value distribution and conditional probability test show the excellent unbiased performance of the proposed QRNG, and hence the system selects randomly one of its possible output phase states, worked like a perfect optical coin toss. As the bit sequence

of QRNG directly related to the number of pulses circulating in the DOPO cavity, we expect that the optical bit sequence could be further scaled by extending our DOPO approach. For instance, by increasing the pump repetition frequency and cavity length, the number of pulses in the resonator is multiplied, and higher bit-rate is expected to be achieved. As a simple example, when a 1 GHz Yb-doped laser system is utilized as pump source, as many as 100 bit is achievable in the current scheme with 1 GHz bit rates, the bit sequence could be extending 20 times. Besides, we can refresh the bit sequence at a frequency of more than 1 MHz by using a faster acoustic optical modulator to turn on and off the DOPO. We envision that this work will inspire the creation of novel type multi-bit optical random number and further promote their applications, such as optical computation, optical data storage, and quantum information sciences.

Funding. National Natural Science Foundation of China (62105237, 62227821, 61827821).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. C. Kenny, "Random number generators: an evaluation and comparison of random.org and some commonly used generators," Technical Report (Trinity College Dublin Management Science and Information Systems Studies, 2005), <https://www.random.org/analysis/Analysis2005.pdf>.
2. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.* **89**(1), 015004 (2017).
3. M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Rev. Sci. Instrum.* **78**(4), 045104 (2007).
4. M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, *et al.*, "Photon arrival time quantum random number generation," *J. Mod. Opt.* **56**(4), 516–522 (2009).
5. M. Wahl, M. Leifgen, M. Berlin, *et al.*, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Appl. Phys. Lett.* **98**(17), 171105 (2011).
6. A. Khanmohammadi, R. Enne, M. Hofbauer, *et al.*, "A monolithic silicon quantum random number generator based on measurement of photon detection time," *IEEE Photonics J.* **7**(5), 1–13 (2015).
7. P. J. Bustard, D. Moffatt, R. Lausten, *et al.*, "Quantum random bit generation using stimulated raman scattering," *Opt. Express* **19**(25), 25173–25180 (2011).
8. Y. Q. Nie, L. Huang, Y. Liu, *et al.*, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Rev. Sci. Instrum.* **86**(6), 063105 (2015).
9. C. R. S. Williams, J. C. Salevan, X. Li, *et al.*, "Fast physical random number generator using amplified spontaneous emission," *Opt. Express* **18**(23), 23584–23597 (2010).
10. A. Argyris, E. Pikasis, S. Deligiannidis, *et al.*, "Sub-tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," *J. Lightwave Technol.* **30**(9), 1329–1334 (2012).
11. T. Tomaru, "Continuous-variable random-number generation from an amplified spontaneous emission light source," *Appl. Opt.* **59**(10), 3109–3118 (2020).
12. C. Gabriel, C. Wittmann, D. Sych, *et al.*, "A generator for unique quantum random numbers based on vacuum states," *Nat. Photonics* **4**(10), 711–715 (2010).
13. D. Milovancev, N. Vokic, C. Pacher, *et al.*, "Towards Integrating True Random Number Generation in Coherent Optical Transceivers," *IEEE J. Sel. Top. Quantum Electron* **26**(5), 1–8 (2020).
14. Z. Zheng, Y. Zhang, W. Huang, *et al.*, "6 Gbps real-time optical quantum random number generator based on vacuum fluctuation," *Rev. Sci. Instrum.* **90**(4), 043105 (2019).
15. F.-X. Wang, C. Wang, W. Chen, *et al.*, "Robust Quantum Random Number Generator Based on Avalanche Photodiodes," *J. Lightwave Technol.* **33**(15), 3319–3326 (2015).
16. H. Fürst, H. Weier, S. Nauerth, *et al.*, "High speed optical quantum random number generation," *Opt. Express* **18**(12), 13029–13037 (2010).
17. M. Jankowski, A. Marandi, C. R. Phillips, *et al.*, "Temporal simulators in optical parametric oscillators," *Phys. Rev. Lett.* **120**(5), 053904 (2018).
18. A. Roy, S. Jahani, C. Langrock, *et al.*, "Spectral phase transitions in optical parametric oscillators," *Nat. Commun.* **12**(1), 835 (2021).
19. A. Roy, R. Nehra, S. Jahani, *et al.*, "Temporal walk-off induced dissipative quadratic solitons," *Nat. Photonics* **16**(2), 162–168 (2022).
20. B. Lu, C. -R Fan, L. Liu, *et al.*, "Speed-up coherent Ising machine with a spiking neural network," *Opt. Express* **31**(3), 3676–3684 (2023).
21. A. Marandi, N. C. Leindecker, K. L. Vodopyanov, *et al.*, "All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators," *Opt. Express* **20**(17), 19322–19330 (2012).

22. T. Steinle, J. N. Greiner, J. Wrachtrup, *et al.*, “Unbiased all-optical random-number generator,” *Phys. Rev. X* **7**(4), 041050 (2017).
23. A. Viotti, M. Seidel, E. Escoto, *et al.*, “Multi-pass cells for post-compression of ultrashort laser pulses,” *Optica* **9**(2), 197 (2022).
24. C. Dietrich, I. Babushkin, J. Andrade, *et al.*, “Field enhancement in a doubly resonant optical parametric oscillator,” *Opt. Lett.* **44**(19), 4909–4912 (2019).
25. Y. S. Cheng, R. A. McCracken, and D. T. Reid, “Dither-free stabilization of a femtosecond doubly resonant OPO using parasitic sum-frequency mixing,” *Opt. Lett.* **45**(3), 768–771 (2020).
26. G. Niestegge, “An approach to quantum mechanics via conditional probabilities,” *Found Phys* **38**(3), 241–256 (2008).