Unbiased All-Optical Random-Number Generator

Tobias Steinle,[1,2,†] Johannes N. Greiner,[2,3] Jörg Wrachtrup,[2,3,4] Harald Giessen,[1,2] and Ilja Gerhardt[2,3,4,*]

[1]*University of Stuttgart, 4th Physics Institute and Research Center SCoPE, Pfaffenwaldring 57, 70569 Stuttgart, Germany*

[2]*Center for Integrated Quantum Science and Technology, IQST, Pfaffenwaldring 57, 70569 Stuttgart, Germany*

[3]*University of Stuttgart, 3rd Physics Institute and Research Center SCoPE, Pfaffenwaldring 57, 70569 Stuttgart, Germany*

[4]*Max Planck Institute for Solid State Research, Heisenbergstraße 1, 70569 Stuttgart, Germany*

(Received 13 June 2017; revised manuscript received 8 August 2017; published 30 November 2017)

The generation of random bits is of enormous importance in modern information science. Cryptographic security is based on random numbers which require a physical process for their generation. This is commonly performed by hardware random-number generators. These often exhibit a number of problems, namely experimental bias, memory in the system, and other technical subtleties, which reduce the reliability in the entropy estimation. Further, the generated outcome has to be postprocessed to "iron out" such spurious effects. Here, we present a purely optical randomness generator, based on the bistable output of an optical parametric oscillator. Detector noise plays no role and postprocessing is reduced to a minimum. Upon entering the bistable regime, initially the resulting output phase depends on vacuum fluctuations. Later, the phase is rigidly locked and can be well determined versus a pulse train, which is derived from the pump laser. This delivers an ambiguity-free output, which is reliably detected and associated with a binary outcome. The resulting random bit stream resembles a perfect coin toss and passes all relevant randomness measures. The random nature of the generated binary outcome is furthermore confirmed by an analysis of resulting conditional entropies.

DOI: 10.1103/PhysRevX.7.041050 Subject Areas: Optics

I. INTRODUCTION

Random numbers are of utter importance in our everyday life, even if many of us are not into gambling or statistics [1]. The most crucial use of random numbers is strong cryptography—securing modern communication, money transfers, and storage of sensitive information. The encryption keys which are used to unlock encrypted data are secured by mathematical hard problems, most notably the discrete logarithm problem or prime-number factorization. The underlying keys are based on random numbers. As recently shown, one of the most efficient attack vectors on modern cryptography is the supply of weak random numbers [2,3], reducing the key space to a fraction of the mathematical probable: Assuming a modern encryption key with N bits results in a key space of 2^N possibilities—with large N this requires a long time for a brute-force decryption process. When such a key is based on only $n \ll N$ possible outcomes of a random-number generator, the decryption of the data might be a question of seconds.

In the computer age, the first idea that might come to mind is a computer-based randomness generator. Unfortunately, such generators are commonly defined based on a recurrence relation, and can only emit (partially very long) cycles of seemingly random bits [4,5]. Therefore, hardware-based random-number generators were presented in the past. The early hardware random-number generators were a die [1] or simply a coin [6]. Both generators are well known even to nonscientists. In mathematical terms, a coin toss is a Bernoulli trial of the sample space $\Omega = \{\mathbf{0}, \mathbf{1}\}$—at least when the coin is not landing on its edge [7]. A *fair* coin is defined as a model system which exhibits no bias, cannot land on the edge, has no memory, and exhibits the probability $p(\mathbf{0}) = p(\mathbf{1}) = 1/2$. This system is well covered in literature [6,8–10]. Besides classical random bit generators, which have to fulfill a number of requirements [11], a recent development is quantum random-number generators, which utilize the inherently unpredictable nature of quantum effects to deliver random numbers [12–19].

For future applications, electrical circuits may eventually be completely replaced by solely optical devices due to the practical advantages of photons in terms of speed, leakage, heat development, and wiring. Therefore, we introduce an

*Corresponding author.
i.gerhardt@fkf.mpg.de

†Present address: ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain.

"all-optical" randomness generation, in which the random process is independent of a particular detector implementation. A specific example is optical parametric oscillators (OPOs), c, degenerate ones, which were used for this task before [20–22]. The relative phase of two generators results in a two-state outcome—but it requires experimental efforts, such as two phase-stabilized OPOs. As outlined in the literature, the OPO's outcoming phase is based on quantum processes, such that this represents another form of quantum randomness generation [22–28]. The generation of random numbers by an OPO has some advantages: the speed of an optical generator, its equienergetic bistability, as well as a demodulator-based and ambiguity-free measurement principle. By "ambiguity free" we refer to a measurement that has two (or more) definite outcomes, which cannot be confused due to technical issues of the measurement apparatus. In quantum randomness generation with single photon detectors, such ambiguities can occur, for example, due to dead times, electrical jitter, and varying detection efficiencies [29].

Here, we present the use of a bistable configuration implemented in a period-doubling optical parametric oscillator for randomness generation. To the best of our knowledge, this is the first experimental utilization of a period-2 (P2) state in an OPO reported in the literature to date. A simplified model is depicted in Fig. 1. The involved bistability is equienergetic and equiprobable; only two outcomes are possible and no bias is observed. For randomness generation, the stream of binary outcomes can be used directly, and no additional unbiasing or bit extraction is required. We test the outcome against the predicted outcomes of a fair coin toss. At the end of the paper, we compute the most conservative bound, the min entropy, against the size of a finite sample of bits originating from the generator.

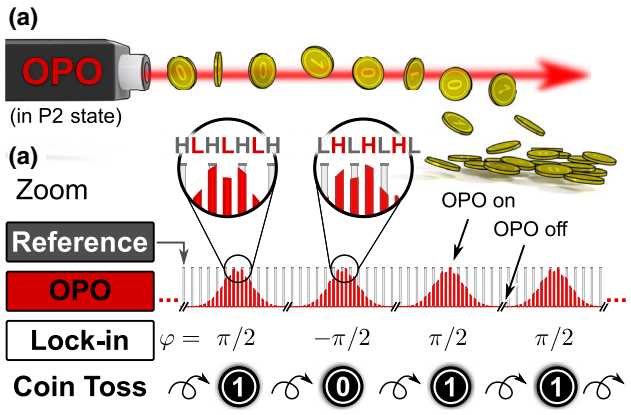

FIG. 1. Operation principle of the all-optical randomness generator. (a) The output of an optical parametric oscillator (OPO) generates two different output states unambiguously. Both outputs are equienergetic and equiprobable, and are based on the transient oscillation of the OPO. We associate the outcomes to an output bit, comparable to a coin toss. (b) The detection is performed by a phase measurement (φ) against an external reference clock, supplied by the pump laser. **H** and **L** denote the different pulse energy outputs of the OPO, which operates in the period-2 state, named P2.

II. EXPERIMENTAL SCHEME

A homebuilt fiber-feedback OPO [30,31] is pumped by a mode-locked 450-fs, 1032-nm Yb:KGW oscillator [Fig. 2(a)]. The gain element is a periodically poled lithium niobate crystal. The repetition rate is defined by the laser and amounts to 40.9 MHz; the length of the OPO cavity is matched to this by a movable mirror. A part of the OPO cavity consists of a single-mode feedback fiber, which in combination with the variable output coupler allows us to control the effective intracavity nonlinearity. The output signal is detected on a reverse-biased InGaAs photodiode (Hamamatsu). The signal is monitored in real time on an oscilloscope [see Fig. 2(c)]. Alternatively, the signal is fed into a lock-in amplifier for further analysis.

When the pump power is varied, the OPO exhibits a bimodal behavior, which can be identified as period doubling [32–36]. Above its oscillation threshold, the OPO operates in the steady state [yellow trace in Fig. 2(b)], which results in an output pulse train with identical subsequent pulses, as known from any mode-locked laser. Upon further increase of pump power, the system enters the so-called period-2 state, which delivers alternating pulses with different pulse energy, peak power, and spectral properties. This behavior originates from the interplay of spectral selective gain and nonlinear feedback [37]. As a result of the synchronous pumping of the OPO, these pulses are temporally aligned with the pump frequency.

When the pump frequency (40.9 MHz in this case) is electronically divided by 2, the pulse train in the P2 state has a defined phase against this derived reference signal. When the OPO is turned on, this phase may be either in phase or, with 50% probability, out of phase. This phase difference of π can be unambiguously measured with various demodulation techniques. A simple and convenient way is the relative multiplication between the detected signal and the reference. A simple commercial solution is the detection with a lock-in amplifier, which allows for a direct access to the relative phase φ. Here, a Zurich Instruments lock-in amplifier is used (UHFLI). The measurement time to determine the phase amounts to 1 μs.

For random-number generation, the OPO is turned on and off by an optical chopper, which is installed such that it can inhibit the cavity oscillation. Figure 2(c) shows the sequence of generating one single bit in the generator: The measured signal (red) is measured versus the reference signal (REF), which corresponds to half of the repetition rate of the pump laser (f_{rep}). This measurement is performed twice in one chopper cycle: when the OPO is off—as the control signal—and when the OPO is in the P2 state—as the signal of the running oscillator, the tossed and

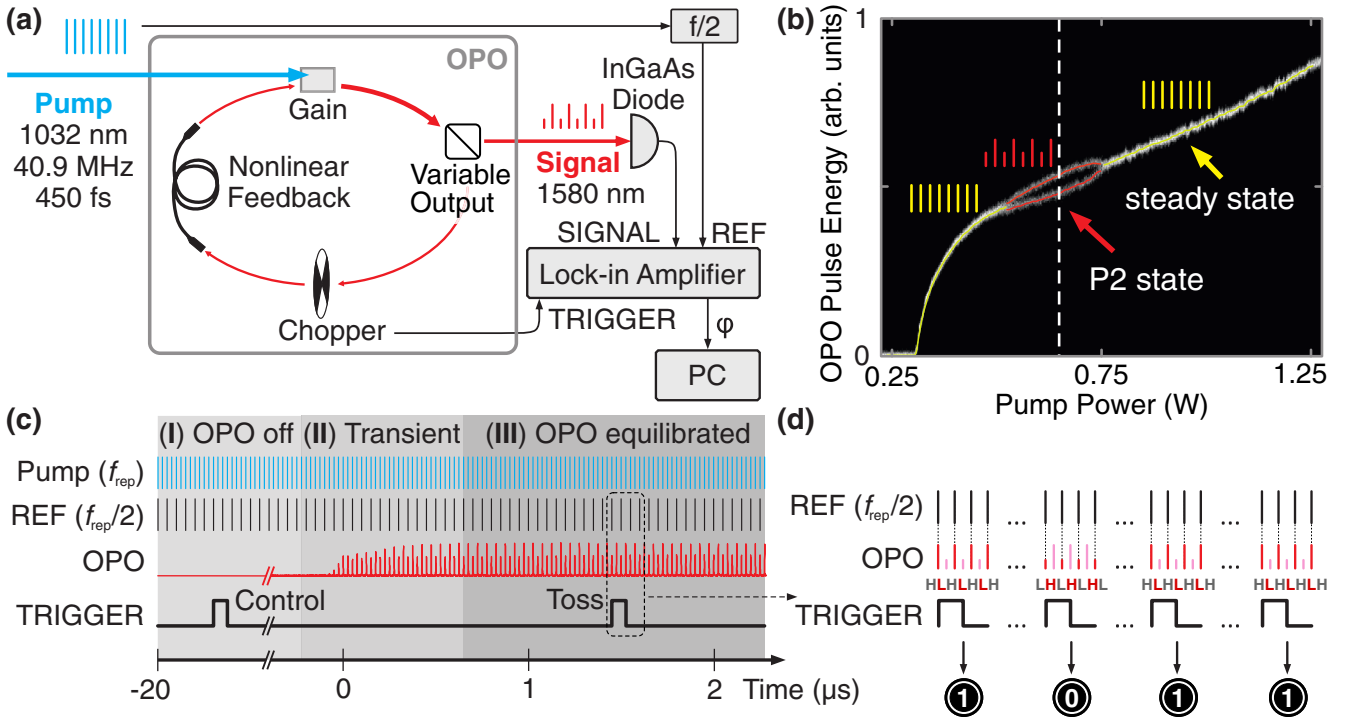

FIG. 2. Experimental scheme of randomness generation. (a) Experimental implementation of the optical parametric oscillator. (b) Power-dependent output pulse energy. Note that both different output pulse train options are equienergetic. (c) Measured transition scheme, periodic with the chopper frequency. The trigger pulse defines two measurements: one when the OPO is blocked (control), and one when the P2 regime is reached (toss). The reference frequency is 40.9 MHz/2, supplied by the pump laser and a frequency divider. (d) Interpretation of measurement outcomes as final bits.

landed coin. The control measurement is performed to verify that two subsequent measurements do not carry spurious information from one to the next outcome. A sequence of four consecutive measurements in the on state is depicted in Fig. 2(d). H and L denote the two alternating, high and low, pulse energy outputs of the OPO in the P2 state, respectively.

The measurement outcome is saved by a MATLAB (Matlab, Inc.) script into a comprehensive set of data, which saves all measured phases. These can be either analyzed as direct phases or, alternatively, processed as bit outcomes.

The measured phase of the oscillating OPO exhibits essentially two measurement outcomes: $-\pi/2$ and $\pi/2$. By means of a simple threshold, the measurements are selected into a binary outcome. Values above zero phase are associated with the outcome **1**, whereas values below zero are assigned a value of **0**. Equally, these outcomes are the two possible stable configurations of the P2 state, L**H**L**H**… (**0**) or H**L**H**L**… (**1**), where the order is fixed by the reference signal, at half of the pump frequency [see Fig. 2(d)]. In the description above, a bold character denotes that the pulse from the OPO is not coinciding with the reference pulse train. This corresponds to a (red) colored character in Fig. 1 or 2. The measurement results are plotted in a histogram, and exhibit a very narrow distribution around the estimated value [see Fig. 3(b)].

III. ORIGIN OF RANDOMNESS

It is well established in the literature that the randomness element in the transient process of a starting OPO originates from quantum effects. These include vacuum fluctuations in the gain element as well as cavity losses [22–28]. The primary quantum process in the buildup of the oscillation is the generation of single photons in a spontaneous down-conversion process caused by pumping the nonlinear gain crystal [22,27,28]. The exact contribution of these processes to the formation of the P2 state is currently under investigation. In the context of randomness generation, it is important to note that the period-doubling attractor is, in particular, not a chaotic attractor [38,39]. This is despite the fact that period doubling and chaos might occur in one and the same nonlinear system, as outlined in detail in the Supplemental Material [40].

The independence of the primary randomness process against small fluctuations of the pump power is a crucial feature. In order to demonstrate this peculiarity, we perform numerical pulse propagation simulations (RP Pro Pulse from RP Photonics) of the transient process with an artificially fixed additional seed. These show that a relative intensity change of more than $\pm 1\%$ is required to induce a phase change by π in the measured outcome. However, the measured relative intensity noise [41] integrated from 10 kHz to 20 MHz amounts to $\pm 0.0215\%$ and is thus

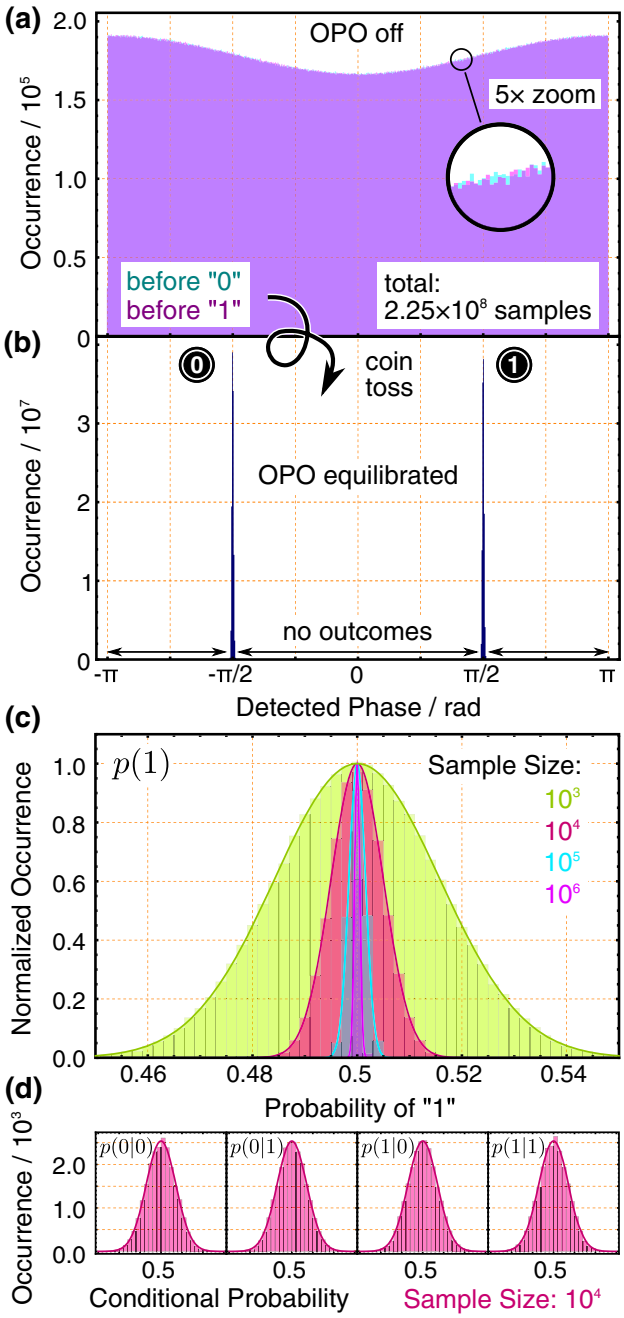

FIG. 3. Analysis of the raw bits. (a) Measurement outcomes when the OPO is off. Essentially, all different phases are randomly measured, with a small bias. (b) Measurement outcomes, after the OPO is equilibrated in the P2 state. (c) Probability to find a 1 as the outcome for different sample sizes N. Note that the solid curve is the predicted result and not a fit. (d) Conditional probability for the different options of tuple outcomes. Range spans from $p_{\mathrm{cond}} = 0.47$ to 0.53. These probabilities are the relevant key figures for the entropy estimation below. Total sample size for all of the above is 2.25×10^8 measurements.

approximately a factor of 50 too low to be the relevant driver of the randomness generation.

Moreover, the independence of subsequent measurement outcomes is important, as discussed on the observed bits below. Therefore, the interbit waiting time is reduced in an additional experiment by a factor of 1000. This is performed with the OPO operated in an extended cavity configuration, such that four independent pulses oscillate simultaneously in the cavity. A subsequent measurement reads four bits within a single chopper cycle. This reduces the relevant time scale for the comparison of successive bits from 100 μs to 100 ns and thus eliminates the contribution of mechanical vibrations, chopper jitter, thermal effects, and pump intensity noise. Nevertheless, we measure alternating bits, which would not be the case if any of the above technical effects would cause the randomness (see Supplemental Material [40]). These investigations indicate that quantum effects are a significant source of randomness in our system.

In order to further quantify the randomness this process produces, we analyze the measured phase and its binary representation for a large set of outcomes in the next section.

IV. FROM RAW BITS TO FINAL BITS

The first analysis of the acquired data involves the measured phase φ of the OPO in its off state. Figure 3(a) shows a histogram of the raw phase output of the lock-in, right before each measurement of the running OPO. The output numbers are divided into outcomes which preceed a zero or a one, respectively. Evidently, both data sets are very similar, and do not show any particular preference for subsequent outcomes. The small bias (wavy curve) is based on spurious signals reaching the lock-in amplifier and is symmetric for both phase outcomes.

After the transient time has passed, a second measurement determines the final state (OPO on). As above, this is analyzed by the lock-in amplifier, resulting in a histogram of events. Both possible outcomes are centered around $-\pi/2$ and $\pi/2$, respectively. Their distribution is determined by experimental uncertainty to measure the phase. This results from spurious phase information, spontaneous down-conversion in the crystal, the sampling and measurement time, and residual (phase) noise in the signal. The width of the determined outcomes (1σ) amounts to 0.0023 rad. In other words, the outcomes are separated by more than 400 standard deviations—excluding the possibility that the two outcomes are confused. Such ambiguity-free measurements cannot be achieved in generators that are based on photon counting due to, e.g., dark counts [12,29,42].

In the course of approximately 1 day a number of $2 \times 2.25 \times 10^8$ measurements are performed. We now analyze a possible bias or imbalance of the experimental outcomes, caused, for example, by technical noise [43]. This noise would produce additional measurement outcomes, which in information theoretical terms add up to the randomness in the transient process of the generator. For the analysis, the bit stream is divided into substrings of length N, and the experimental probability of the outcome 1 is determined.

The distribution is centered around 0.5, independently of the sample size N. The analysis reconfirms the width of the distribution as $\sigma_{\text{single}} = \sqrt{Np(1-p)}/N$. Note that the data are not fitted, but the theoretical curve is depicted along with the measured data.

The balance of the measurement outcomes is only one indication of a well-balanced coin toss. Another important measure is the *conditional* probability, which signifies whether subsequent outcomes contain some form of memory of the prior state of the oscillator. For this, a first indication is given by the analysis of Figs. 3(a) and 3(b)—still, this does not prove the independence of the outcomes of subsequent measurements in the equilibrated OPO. The conditional probability of obtaining the result **1** after a preceding result **0** is denoted as $p(\mathbf{1}|\mathbf{0})$, reading as the probability of one conditioned on zero. This is defined as $p(x|y) = p(x \wedge y)/p(y)$, and is depicted in Fig. 3(c) along with the theoretical prediction of its distribution $\sigma_{\text{cond}} = 1/\sqrt{2N}$. An autocorrelation analysis, which also accounts for higher-order bit-to-bit correlations, is given in the Supplemental Material [40]. Again, the expected behavior is reconfirmed and no memory in the system is evident.

Very common is the use of so-called *random-number tests*. The tests *ent*, the *NIST test suite* [44], the *die-harder* suite, or the most comprehensive *TestU01* suite [45] are commonly known. Many people still believe that such tests are able to show whether a bit string is random or not. But they can only deliver the proof that no substantial flaw occurred in the implementation of a random bit generator. Moreover, most of these tests are based on algorithmic information theory and are designed to test algorithmically generated pseudorandom numbers rather than random numbers generated by physical processes [46]. Therefore, the statement that a certain bit string passes all tests does not prove the random nature of the input. Nonrandom and predictable numbers, such as the binary expansion of π, pass all these tests flawlessly. As expected, our presented generator passes all these tests, and a sample output for the NIST suite is presented in the Supplemental Material [40].

A subset of the described random number tests is the analysis of different bit patterns and their occurrence in the data set. This approach has been examined in early discussions on random-number testing [4]. Nowadays, other authors suggest the use of information theoretic language for random-number testing [46]. In this context, the *coin tossing constants* by Feller [6], which are closely related to the generalized Fibonacci numbers [8], describe the asymptotic probability $p(n,k)$ of the event that a sequence with the length k of **1** or **0** does *not* occur in a sequence of n tosses of a fair coin. Feller's constants have the property

$$\lim_{n\to\infty} p(n,k)\alpha_k^{n+1} = \beta_k. \tag{1}$$

Table I displays the analysis of substrings of length $N = 400$ bits of the generator. This small number is chosen to have nonvanishing values for the probabilities associated with higher-order parameters ($k > 5$). The experimentally determined value is given in the third column, and the relative deviation of the order of 10^{-4} corresponds to the square root (shot noise) of 2.25×10^8 recorded bits. The computed values of the coin tossing constants match very well to the assumed behavior of the supplied random bit sequence.

TABLE I. Feller's coin tossing constants. The constants are related to the probability that a certain sequence of **1**'s does not occur in a set of random bits. Here, the sample size is $N = 400$. The ideal value of the coin tossing constant α is compared to the values extracted from our experimental data. Relative change is calculated as $(\alpha_{\text{ideal}} - \alpha_{\text{extracted}})/\alpha_{\text{ideal}}$. The relative uncertainty is given by the finite length of the acquired data set.

k	α_{ideal}	$\alpha_{\text{extracted}}$	Relative change
2	1.236 067 98	...	...
3	1.087 378 03	...	...
4	1.037 580 13	1.036 763 54	$7.87010735 \times 10^{-4}$
5	1.017 320 78	1.017 314 06	$6.61125775 \times 10^{-6}$
6	1.008 276 52	1.008 279 33	$-2.78877013 \times 10^{-6}$
7	1.004 034 11	1.004 037 01	$-2.88459780 \times 10^{-6}$
8	1.001 988 36	1.001 985 88	$2.47363715 \times 10^{-6}$
9	1.000 986 24	1.000 985 84	$4.01117501 \times 10^{-7}$
10	1.000 490 92	1.000 491 82	$-8.99357769 \times 10^{-7}$
11	1.000 244 86	1.000 246 24	$-1.38152744 \times 10^{-6}$
12	1.000 122 26	1.000 123 58	$-1.31441456 \times 10^{-6}$
13	1.000 061 09	1.000 061 63	$-5.40416736 \times 10^{-7}$
14	1.000 030 53	1.000 030 25	$2.79986856 \times 10^{-7}$
15	1.000 015 26	1.000 015 22	$4.33916550 \times 10^{-8}$

The coin tossing constants analyze higher orders of tuples than the conditional probability and are therefore similar in this respect to a mathematical Borel *normality* test [4], which analyzes the lexicographical occurrence of all possible binary strings. Such a test was implemented by Calude *et al.* for testing a number of hardware-based randomness generators [47].

The above analysis on the probability of subsequent sets of measurement outcomes underlines the behavior of an ideal coin toss. An interesting effect occurs when we process the measurement outcomes by pairing each bit with exactly one neighboring bit, without allowing any overlaps of the tuples—unlike as before. Although we find all tuple permutations (**00**, **01**, **10**, **11**) to be equally probable, the waiting time, which is the "distance" between two equivalent outcomes, is different between the bit-changing (**01**, **10**) and bit-equivalent outcomes (**00**, **11**). For the tuples including a bit flip, the predicted waiting time is 4 consecutive tosses. On the other hand, a double sequence of **00**, or **11**, has a predicted waiting time of 6 consecutive tosses. This is verified with the present set of data and we determine values of 3.999 76 and 5.997 84, respectively. Again, the relative uncertainty of approximately 10^{-4} corresponds to the length of the data set; it proves that there is no further memory storage in the

measurement outcomes and reconfirms the predicted behavior.

In summary, we conclude that the measured raw bits of the presented all-optical randomness generator using a nonlinear feedback OPO in the P2 state do not differ by any measurable means from the ones of a perfect Bernoulli trial. This is indicated by the independence of consecutive measurement outcomes, the balance between the two probabilities, and further tests, which resemble the expected outcomes of a perfect coin toss. Subsequently, the required postprocessing can be reduced to a minimum. Such a postprocessing would generally be required for any physical implementation of a fair (perfect) coin toss due to finite-size effects. We now turn to the entropy analysis of the raw bit stream.

V. ENTROPY ESTIMATION

While all above measures suggest that the raw bits are usable as a perfect source of random bits, we have ignored an important information theoretical measure of the output of the experimental apparatus so far: the generated entropy. As we outline below, the crucial quality figure for a randomness generator is the achievable entropy per output bit. Ideally, each bit has the perfect entropy of unity, which means that each generated bit can be used as an independent optical coin toss and resembles the output of a fair coin. But when a finite fraction of bits is analyzed, this can only be proven if all **1**'s and **0**'s are equally balanced. Intrinsically, there might be an unwanted (but statistically allowed) bias. In this case, the determined entropy will be lower than one. Because of the finite length, this is most likely the case for the presented data set. A first naive approach to calculate the entropy analyzes the balance of the bit stream, and is given by the unconditional Shannon entropy, which is defined as

$$\mathcal{H}_{\mathrm{Sh}} = \sum_y p(y) I(p(y)) = -\sum_y p(y) \log_2 p(y), \quad (2)$$

where $p(y)$ is the single probability of obtaining **0** or **1** in the full bit sequence, respectively. This, however, does not consider any dependence or memory effects in the measurement outcomes, where, for example, an alternating sequence **101010**… would result in the same entropy as a fully random, i.e., totally unordered, sequence. Therefore, the *conditional* entropy is considered, accounting for the memory (or the absence thereof) in the system. This is defined as

$$\begin{aligned}\mathcal{H}_{\mathrm{Sh}}(X|Y) &= \sum_y p(y) \mathcal{H}_{\mathrm{Sh}}(X|Y=y) \\ &= -\sum_y p(y) \sum_x p(x|y) \log_2 p(x|y). \end{aligned} \quad (3)$$

See the Supplemental Material [40] for details of our calculation of the conditional entropy. We mention for clarity that the events y and x are defined as "the ith bit is **0**(**1**)" and "the $(i+1)$th bit is **0**(**1**)." Uppercase Y and X are the unified sets of events on all bits. Thus, our notion of entropy is linked to the frequency analysis of output data, but can also be estimated *a priori*. Unlike the Shannon entropy, the min entropy (denoted as $\mathcal{H}_\infty$) is the most conservative bound for the usable entropy of a randomness generator. It maximizes the (conditional) probability $p(x|y)$ against x. This imbalance and maximizing effect can be seen in Figs. 3(c) and 3(d). It becomes evident that, for a larger sample size N, the width of the distribution shrinks and the amount of entropy is commonly larger. The min entropy is defined as

$$\mathcal{H}_\infty(X|Y) = -\log_2 \left[\sum_y p(y) \max_x \{ p(x|y) \} \right]. \quad (4)$$

The above entropy definitions can be straightforwardly computed for an experimentally generated data set. This results in a scalar entropy value, which still has to be interpreted; for a good generator, the resulting number will usually be close to one. How "perfect" the entropy is and how close it reaches to one depends on three factors: (a) the quality of the generator, (b) the size of the analyzed bit stream (here denoted as N for the number of analyzed bits), and (c) which particular data set is analyzed. Conclusively, it is very unlikely to achieve an entropy of unity when the entropy for a finite bit string is computed. This even holds for a fair coin. In the following, we perform an analysis of the generator's outcome and compute if the entropy matches the predicted value.

Figure 4 shows the calculated Shannon and min entropy for the presented data set against the sample size N. Note that this graph shows the deviation against perfect entropy on a logarithmic scale. For a *smaller* sample size N (left-hand side), a larger number of samples exist, and more points are depicted. As mentioned before, with a *larger* sample size N, the entropy approaches unity. The conditional Shannon entropy scales linearly with N, whereas the min entropy is proportional to $\sqrt{N}$. The value and the distribution of the min entropy are significantly smaller than for the Shannon entropy, since the conditional probability is maximized. Figure 4 also shows entropy bounds which are obtained *a priori*. These include the second highest possible value of the entropy for a certain sample size, besides the ideal case of perfect entropy. This is the highest value that can occur when a minimally entropy-changing single bit flip is present in a data set of length N. These curves scale quadratic against the mean slope behavior, which we introduce above. Therefore, the mean value for the conditional Shannon entropy forms a parallel line to the highest min entropy, where one bit flip is present.

The min entropy is a conservative bound and selects the maximal conditional probability in a set of random bits. If a perfect random string is infinitely long, every possible occurrence will show up in a subset of this sequence.

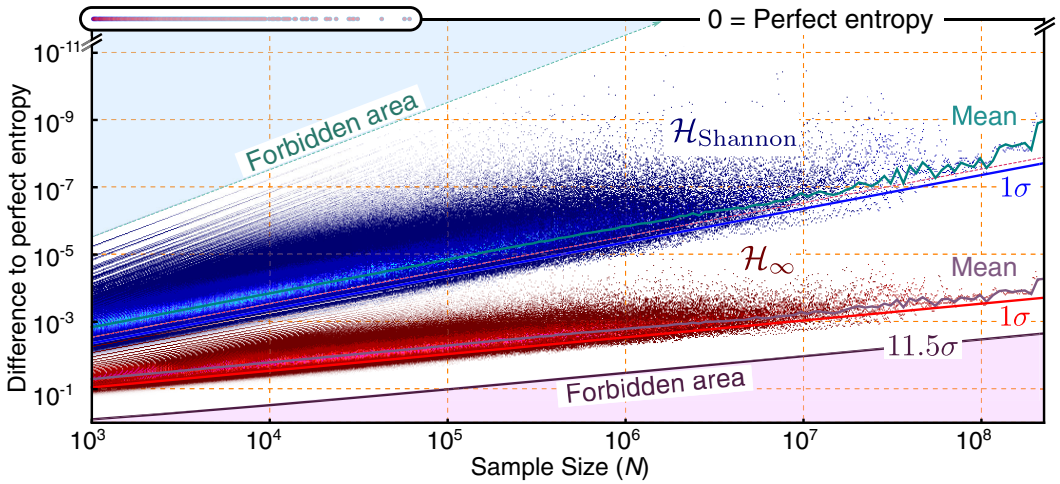

FIG. 4. Final entropy in the generated bit stream. The difference of the entropy ($\mathcal{H}$) to unity is shown for the Shannon entropy (blue) and min entropy (red) against the sample size (N). A higher density and brighter color of the points obtained from experimental data signifies more outcomes of a certain value. The best possible case is a difference of 0, as displayed after a cutoff of the logarithmic scale on top of the graph. For $N < 10^5$, sequences possessing this "perfect" entropy are still observed, shown as separate points. If a specific single bit is flipped, the entropy is reduced below unity. Subsequently, points in the graph that do not exhibit unity entropy cannot be higher than a certain limit (dashed curve). This forms a forbidden area to the top with no mathematically possible outcome. The solid straight line at the bottom indicates the conservative bound. These bounds are obtained *a priori* by an error propagation on the entropy of a fair coin, as outlined in the Supplemental Material [40]. Red: 1σ deviation from the expected min entropy. Purple: Assuming an outlier probability of 2^{-100}. As expected, no values are found below this line.

Then, in contradiction to the description above, a set of calculated entropies would eventually be very small since a very long sequence of seemingly nonrandom bits can occur (e.g., such as **1111111**…). For these cases, the calculated entropy may be reduced to zero. For realistic considerations it is therefore important to exclude, for instance, such infinitesimally likely events of all bits of a long sequence being **1**. Such a calculation of the occurrence of a certain set of equivalent outcomes of a generator is presented in the calculation of the coin tossing constants above (Table I). Additionally, a possible error bound for randomness extraction was introduced by Troyer and Renner [48] as $1/2^{100} \approx 1/10^{30}$. Such bounds are also described to guarantee an "ϵ randomness" [43]. The proposed bound of $1/2^{100}$ ensures that 1×10^6 generators do not have the option to exhibit the same outcome (i.e., a so-called *collision* of two generators) in the age of the Universe. In the case of Gaussian distributed events, this corresponds to approximately 11.5 standard deviations from the center of the distribution. Figure 4 shows this bound as the lowest curve, obtained *a priori* by an error propagation on the entropy of a fair coin, as outlined in the Supplemental Material [40]. As suggested from the raw bit analysis, no selected subset of the bits falls below this line—this suggests that the model of a perfect coin toss seems to be appropriate for the introduced generator.

For our presented sample size of 2.25×10^8, the conditional min entropy per bit can be estimated as 99.95%. This can be simply read from Fig. 4 on the right-hand side. This value is, of course, solely limited by the finite sample volume. The most conservative bound (11.5σ) of the entropy difference to unity is approximately 1 order of magnitude different, and the entropy amounts to 99.5%.

With the raw bits, as discussed above, but also by merit of the calculated entropies, we are able to prove that the recorded bit stream does not differ by any measurable means from a perfect coin toss. Each emitted bit can therefore be used as a random bit. No further randomness extraction has to be considered when a large enough bit string is used. Of course, we are only able to prove this assumption bound to the size of the recorded bit string.

VI. CONCLUSION AND OUTLOOK

We present an unbiased all-optical coin toss. It is based on the bistable outcome of an optical parametric oscillator with nonlinear fiber feedback, operating in the P2 state. The detection scheme relies on phase detection versus an external reference pulse. This implementation is substantially simpler than prior published experiments [20–22], since it does not require degenerate operation of the OPO. The disadvantage of degenerate operation is that it necessitates either an actively interferometrically stabilized resonator to fix the relative optical phases of the signal and idler frequency combs to the pump frequency comb or a "shaker" using a "dither and lock" algorithm that periodically varies the cavity length to generate an error signal for the stabilization. This introduces noise to the system which can be avoided by a nondegenerate operation.

The implemented detection scheme, based on period doubling, is ambiguity free, i.e., has only two possible outcomes, separated by more than 400 standard deviations, which can be interpreted as zeros and ones of a random bit sequence. This uniquely decouples the fundamental randomness process from the detection principle. While the detection here is based on a lock-in amplifier, more simple schemes can be developed. A demodulator or a radio-frequency mixer and a comparator will reduce the implementation costs, and emit the random sequence directly into an, e.g., logic level output.

One limitation is given by the sample rate of the chopper, which is limited to 10 kHz in the presented design. This sample rate is ultimately limited by the transient process until the OPO is in a stable state and the required time for phase detection. The measurement time to determine the phase amounts to 1 μs with the current detection system. This may be shortened in future experiments by a factor of 10. Accordingly, a faster chopper can be installed as well. As evident in Fig. 2(c), we estimate the time for equilibration to approximately 300 ns and the ambiguity-free detection of the phase state to 2–3 cycles, amounting to 100–150 ns. With the described OPO, and by introducing a faster chopper, a random bit rate above 1 MHz can be reached. An even further speed-up can be implemented with a higher repetition rate of the pump laser. For such changes, OPOs reaching the GHz range are reported [49]. As a side effect, this would result in a much more compact design for the entire experimental configuration. Building a more compact randomness generator could further be realized by implementing the introduced principle with state-of-the-art technology on a photonic chip [50–52].

The full quantum mechanical description of the open quantum system, specifically in the P2 state, remains to be addressed in future work. Commonly, the process of a bistable outcome of an OPO is described as a quantum process [22–28], growing from quantum mechanical vacuum fluctuations. A careful analysis on the transient process, which may also introduce a fiber-optic electro-optic modulator instead of a chopper, along with more research on the power dependence will likely characterize this process and the P2 state in further detail. A deeper understanding of the underlying physics might lead to faster phase detection and larger random bit rates, and even to future implementations in quantum information processing and quantum simulation [53].

ACKNOWLEDGMENTS

We acknowledge the support for the 3D rendering by Ingmar Jakobi for Fig. 1. T. S. thanks the Carl Zeiss Foundation. We further acknowledge the funding from the MPG, the BW Stiftung and the DFG, the SFB Project No. CO.CO.MAT/TR21, ERC (Complexplas), the BMBF, the Eisele Foundation, the project Q.COM, and SMel.

T. S. and J. N. G. contributed equally to this work.

[1] F. Galton, *Dice for Statistical Experiments*, Nature (London) **42**, 13 (1890).

[2] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter, *Ron Was Wrong, Whit Is Right*, https://eprint.iacr.org/2012/064.

[3] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, *Stealthy Dopant-Level Hardware Trojans*, in *Cryptographic Hardware and Embedded Systems*, edited by G. Bertoni and J. S. Coron, Lecture Notes in Computer Science Vol. 8086 (Springer, New York, 2013), pp. 197–214.

[4] D. Knuth, *The Art of Computer Programming: Seminumerical Algorithms* (Addison-Wesley, Reading, MA, 1998), Vol. 2.

[5] H. Bauke and S. Mertens, *Pseudo Random Coins Show More Heads Than Tails*, J. Stat. Phys. **114**, 1149 (2004).

[6] W. Feller, *An Introduction to Probability Theory and Its Applications*, 3rd ed. (Wiley, New York, 1968).

[7] D. B. Murray and S. W. Teare, *Probability of a Tossed Coin Landing on Edge*, Phys. Rev. E **48**, 2547 (1993).

[8] M. Finkelstein and R. Whitley, *Fibonacci Numbers in Coin Tossing Sequences*, Fibonacci Q. **16**, 539 (1978).

[9] J. Ford, *How Random is a Coin Toss*, Phys. Today **36** No. 4, 40 (1983).

[10] V. Z. Vulović and R. E. Prange, *Randomness of a True Coin Toss*, Phys. Rev. A **33**, 576 (1986).

[11] M. Stipčević, *Fast Nondeterministic Random Bit Generator Based on Weakly Correlated Physical Events*, Rev. Sci. Instrum. **75**, 4442 (2004).

[12] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, *Optical Quantum Random Number Generator*, J. Mod. Opt. **47**, 595 (2000).

[13] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, *A Fast and Compact Quantum Random Number Generator*, Rev. Sci. Instrum. **71**, 1675 (2000).

[14] M. Stipčević and B. M. Rogina, *Quantum Random Number Generator Based on Photonic Emission in Semiconductors*, Rev. Sci. Instrum. **78**, 045104 (2007).

[15] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, *High Speed Optical Quantum Random Number Generation*, Opt. Express **18**, 13029 (2010).

[16] R. Colbeck, Quantum and Relativistic Protocols for Secure Multi-Party Computation, arXiv:0911.3814.

[17] S. Pironio, A. Acin, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Random Numbers Certified by Bell's Theorem*, Nature (London) **464**, 1021 (2010).

[18] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, *Quantum Random Number Generation on a Mobile Phone*, Phys. Rev. X **4**, 031056 (2014).

[19] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, *True Random Numbers from Amplified Quantum Vacuum*, Opt. Express **19**, 20665 (2011).

[20] A. Marandi, N. C. Leindecker, V. Pervak, R. L. Byer, and K. L. Vodopyanov, *Coherence Properties of a Broadband Femtosecond Mid-IR Optical Parametric Oscillator Operating at Degeneracy*, Opt. Express **20**, 7255 (2012).

[21] Y. Okawachi, M. Yu, K. Luke, D. O. Carvalho, M. Lipson, and A. L. Gaeta, *Quantum Random Number Generator*

Using a Microresonator-Based Kerr Oscillator, Opt. Lett. **41**, 4194 (2016).

[22] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, *All-Optical Quantum Random Bit Generation from Intrinsically Binary Phase of Parametric Oscillators*, Opt. Express **20**, 19322 (2012).

[23] M. Herrero-Collantes and J. C. Garcia-Escartin, *Quantum Random Number Generators*, Rev. Mod. Phys. **89**, 015004 (2017).

[24] Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto, *Coherent Ising Machine Based on Degenerate Optical Parametric Oscillators*, Phys. Rev. A **88**, 063853 (2013).

[25] P. D. Drummond, K. Dechoum, and S. Chaturvedi, *Critical Quantum Fluctuations in the Degenerate Parametric Oscillator*, Phys. Rev. A **65**, 033806 (2002).

[26] C. D. Nabors, S. T. Yang, T. Day, and R. L. Byer, *Coherence Properties of a Doubly Resonant Monolithic Optical Parametric Oscillator*, J. Opt. Soc. Am. B **7**, 815 (1990).

[27] S. E. Harris, M. K. Oshman, and R. L. Byer, *Observation of Tunable Optical Parametric Fluorescence*, Phys. Rev. Lett. **18**, 732 (1967).

[28] W. H. Louisell, A. Yariv, and A. E. Siegman, *Quantum Fluctuations and Noise in Parametric Processes. I*, Phys. Rev. **124**, 1646 (1961).

[29] L. Oberreiter and I. Gerhardt, *Light on a Beam Splitter: More Randomness with Single Photons*, Laser Photonics Rev. **10**, 108 (2016).

[30] T. Südmeyer, J. A. der Au, R. Paschotta, U. Keller, P. G. R. Smith, G. W. Ross, and D. C. Hanna, *Femtosecond Fiber-Feedback Optical Parametric Oscillator*, Opt. Lett. **26**, 304 (2001).

[31] T. Steinle, F. Neubrech, A. Steinmann, X. Yin, and H. Giessen, *Mid-Infrared Fourier-Transform Spectroscopy with a High-Brilliance Tunable Laser Source: Investigating Sample Areas Down to* 5 μm *Diameter*, Opt. Express **23**, 11105 (2015).

[32] K. Ikeda, *Multiple-Valued Stationary State and Its Instability of the Transmitted Light by a Ring Cavity System*, Opt. Commun. **30**, 257 (1979).

[33] L. Lugiato, C. Oldano, C. Fabre, E. Giacobino, and R. Horowicz, *Bistability Self-Pulsing and Chaos in Optical Parametric Oscillators*, Nuovo Cimento Soc. Ital. Fis. **D10**, 959 (1988).

[34] C. Richy, K. Petsas, E. Giacobino, C. Fabre, and L. Lugiato, *Observation of Bistability and Delayed Bifurcation in a Triply Resonant Optical Parametric Oscillator*, J. Opt. Soc. Am. B **12**, 456 (1995).

[35] G. Steinmeyer, D. Jaspert, and F. Mitschke, *Observation of a Period-Doubling Sequence in a Nonlinear Optical Fiber Ring Cavity Near Zero Dispersion*, Opt. Commun. **104**, 379 (1994).

[36] M. Kues, N. Brauckmann, T. Walbaum, P. Groß, and C. Fallnich, *Nonlinear Dynamics of Femtosecond Supercontinuum Generation with Feedback*, Opt. Express **17**, 15827 (2009).

[37] N. Akhmediev, J. M. Soto-Crespo, and G. Town, *Pulsating Solitons, Chaotic Solitons, Period Doubling, and Pulse Coexistence in Mode-Locked Lasers: Complex Ginzburg-Landau Equation Approach*, Phys. Rev. E **63**, 056602 (2001).

[38] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, *Fast Physical Random Bit Generation with Chaotic Semiconductor Lasers*, Nat. Photonics **2**, 728 (2008).

[39] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, *An Optical Ultrafast Random Bit Generator*, Nat. Photonics **4**, 58 (2010).

[40] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevX.7.041050 for details on the experimental setup, additional randomness measures, the entropy calculation, and the in-depth calculation of Feller's coin tossing constants.

[41] T. Steinle, F. Mörz, A. Steinmann, and H. Giessen, *Ultra-Stable High Average Power Femtosecond Laser System Tunable from 1.33 to* 20 μm, Opt. Lett. **41**, 4863 (2016).

[42] K. Svozil, *Three Criteria for Quantum Random-Number Generators Based on Beam Splitters*, Phys. Rev. A **79**, 054306 (2009).

[43] M. W. Mitchell, C. Abellan, and W. Amaya, *Strong Experimental Guarantees in Ultrafast Quantum Random Number Generation*, Phys. Rev. A **91**, 012314 (2015).

[44] L. Bassham *et al.*, NIST Report No. SP 800-22 Rev. 1a, 2010, https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final.

[45] P. L'Ecuyer and R. Simard, *Testu01: A C Library for Empirical Testing of Random Number Generators*, ACM Trans. Math. Softw. **33**, 22:1 (2007).

[46] C. S. Calude, *Information and Randomness: An Algorithmic Perspective*, 2nd ed. (Springer, New York, 2010).

[47] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, *Experimental Evidence of Quantum Randomness Incomputability*, Phys. Rev. A **82**, 022102 (2010).

[48] M. Troyer and R. Renner, ID Quantique SA, Carouge Internal Report, 2012, http://marketing.idquantique.com/acton/attachment/11868/f-004d/1/-/-/-/-/quantis-rndextract-techpaper.pdf.

[49] J. M. Roth, T. G. Ulmer, N. W. Spellmeyer, S. Constantine, and M. E. Grein, *Wavelength-Tunable 40-GHz Picosecond Harmonically Mode-Locked Fiber Laser Source*, IEEE Photonics Technol. Lett. **16**, 2009 (2004).

[50] J. Niehusmann, A. Vörckel, P. H. Bolivar, T. Wahlbrink, W. Henschel, and H. Kurz, *Ultrahigh-Quality-Factor Silicon-on-Insulator Microring Resonator*, Opt. Lett. **29**, 2861 (2004).

[51] B. Kuyken, X. Liu, R. M. Osgood, R. Baets, G. Roelkens, and W. M. J. Green, *A Silicon-Based Widely Tunable Short-Wave Infrared Optical Parametric Oscillator*, Opt. Express **21**, 5931 (2013).

[52] C. Abellan, W. Amaya, D. Domenech, P. M. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, *Quantum Entropy Source on an InP Photonic Integrated Circuit for Random Number Generation*, Optica **3**, 989 (2016).

[53] T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P. L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K.-i. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue, *A coherent Ising machine for 2000-node optimization problems*, Science **354**, 603 (2016).