SCIENCE CHINA
Information Sciences

• Supplementary File •

Photonic reservoir computing based min-entropy evaluation for random number generators

Jianjiang WANG[1,2,3,4], Qiang CAI[5], Jianguo ZHANG[1], Pu LI[2,3,4*], K. Alan SHORE[6], Yuwen QIN[2,3,4] & Yuncai WANG[2,3,4]

[1]*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan* 030024*, China;*
[2]*Institute of Advanced Photonics Technology, School of Information Engineering, Guangdong University of Technology, Guangzhou* 510006*, China;*
[3]*Key Laboratory of Photonic Technology for Integrated Sensing and Communication, Ministry of Education of China, Guangdong University of Technology, Guangzhou* 510006*, China;*
[4]*Guangdong Provincial Key Laboratory of Information Photonics Technology, Guangdong University of Technology, Guangzhou* 510006*, China;*
[5]*Department of Physics, Taiyuan Normal University, Taiyuan* 030619*, China;*
[6]*School of Computer Science and Electronic Engineering, Bangor University, Wales* LL57 1UT*, UK*

This supplementary document consists of three main sections. In Appendix A, we introduce the five datasets used in this paper, the theoretical model of photonic reservoir computing (PRC), and the min-entropy calculation method. In Appendix B, we present the effects of four structure parameters,which contain the number of virtual node, injection strength, feedback strength, and frequency detuning. We finally determine an optimal set of parameters. In Appendix C, we provide the PRC evaluation results for the five datasets and compare them with National Institute of Standards and Technology Special Publication (NIST SP 800-90B).

Appendix A Theoretical model of the PRC

Appendix A.1 Datasets

We use five representative simulated data sources to train and test the PRC model, including three pseudo random number sequences generated using the Mersenne Twister algorithm: one that satisfies a discrete uniform distribution, one that approximates a discrete uniform distribution, and one that is rounded to integers from a normal distribution. Additionally, we use a M-sequence generated by linear feedback shift registers and a true random number sequence based on white chaos.

For the first four data sources, their theoretical min-entropy can be derived from the known probability distributions. They are generated using the following distribution families adopted in [1] and [2]. For the first three data sources, we generate 40 consecutive sequences, each containing 1 M samples. For the M-sequence, 1 M samples are generated for each stage n (n = 8, 10, 12, 14, 16, 18).

Discrete Uniform Distribution: The samples, drawn from an independent and identically distributed source, are equally likely.

Discrete Near-Uniform Distribution: All samples from an independent and identically distributed source have the same probability, except for one sample which has a higher probability than the others.

Normal Distribution Rounded to Integers: The samples are normal distribution and rounded to integer values, which come from an independent and identically distributed source.

M-sequence: A typical pseudo-random sequence generated by a linear feedback shift register.

For white chaos true random number sequences, we evaluate the min-entropy of the white chaos by retaining n (n = 1, 2, ..., 8) most significant bits (MSBs). Each MSB contains a sample size of 1 M. The white chaos is experimentally generated by optical heterodyning of two external-cavity lasers. More details on white chaos can be found in [3, 4].

Appendix A.2 Simulation model of the PRC

In our work, the whole working process in the reservoir can be modeled by Eq. (A1) and Eq. (A2) [5, 6]:

$$\frac{dE(t)}{dt} = \frac{1+i\alpha}{2}\left\{\frac{G(N(t)-N_0)}{1+\varepsilon\left|E(t)\right|^2}-\frac{1}{\tau_p}\right\}E(t)+\frac{k_f}{\tau_{in}}E(t-\tau)exp(-i2\pi\nu\tau) + \frac{k_{inj}}{\tau_{in}}E_{inj}(t)exp(i2\pi\Delta\nu t)+\sqrt{2\beta N(t)}\chi(t). \tag{A1}$$

* Corresponding author (email: lipu8603@126.com)

$$\frac{dN(t)}{dt} = J - \frac{N(t)}{\tau_s} - \frac{G(N(t)-N_0)}{1+\varepsilon\left|E(t)\right|^2}\left|E(t)\right|^2. \tag{A2}$$

Where $E(t)$ is the complex electric field and $N(t)$ is the average carrier density. The parameter k_f is the feedback strength of the response laser (R-L), and k_{inj} is the injection strength from the drive laser (D-L) to the R-L. ν is the frequency of the free-running R-L, and $\Delta\nu$ is the frequency detuning from the D-L to the R-L. J is the injection current. The linewidth-enhancement factor $\alpha = 5.0$, the carrier density at transparency $N_0 = 1.4 \times 10^{24}$ m^{-3}, the differential gain coefficient $G = 1.414 \times 10^{-12}$ $\mathrm{m}^3\mathrm{s}^{-1}$, the gain saturation coefficient $\varepsilon = 5 \times 10^{-23}$, the internal cavity round-trip time $\tau_{in} = 7.38$ ps, the photon lifetime $\tau_p = 1.92$ ps, the carrier lifetime $\tau_s = 2.5$ ns, and the feedback delay time τ is 50 ns. $\sqrt{2\beta N(t)}\chi(t)$ represents the noise term, where $\chi(t)$ is a Gaussian noise with zero mean and unity variance, while β represents the noise strength. In our simulation, β is set to 4.5×10^{-4} [7]. Considering that the masked input signal is used to modulate the optical signal by phase modulation, the injection field E_{inj} can be described as follows:

$$E_{inj}(t) = \sqrt{I_d} exp(i\pi \boldsymbol{S}(t)), \tag{A3}$$

where I_d is the photon number of continuous-wave output from the D-L, $I_d = 3.757 \times 10^{20}$. $\boldsymbol{S}(t)$ represents the masked input signal.

Appendix A.3 Min-entropy calculation

Prediction-based methods for entropy evaluation predict the next sample based on the hidden relationships in previous samples and evaluate the min-entropy based on the probability of the correct prediction. This approach corresponds to these prediction-based tests in NIST SP 800-90B, namely the Multi Most Common in Window (MultiMCW) predictor, Lag predictor, Multi Markov Model with Counting (MultiMMC) predictor, and LZ78Y predictor [5]. For a fair comparison these four tests from NIST SP 800-90B are thus selected for comparison in our study. Each predictor provides a prediction result when testing the output of entropy source. The min-entropy of the sequence is then calculated based on the probability of correct prediction. Finally, the smallest value among the results obtained from these predictors is selected as the final min-entropy of the entropy source. In our work, we use the first ten samples to predict the eleventh sample and calculate the minimum entropy based on the probability of a correct prediction. Assuming that the sample size of the test set is N, and the number of correct predictions is N_T. We can calculate the prediction accuracy P_r by Eq. (A4):

$$P_r = \frac{N_T}{N} \times 100\%. \tag{A4}$$

We calculate the global predictability and local predictability with the upper bound of the 99% confidence interval. The global prediction probability P_{global} is calculated as shown in Eq. (A5):

$$P_{global} = \begin{cases} 1 - 0.01^{1/N}, & P_r = 0, \\ min(1, P_r + 2.576\sqrt{\dfrac{P_r(1-P_r)}{N-1}}). \end{cases} \tag{A5}$$

The local prediction probability P_{local} is calculated iteratively by Eq. (A6) and Eq. (A7) [2]:

$$0.99 = \frac{1 - x_{10}P_{local}}{(r+1-rx_{10})(1-P_{local})} \times \frac{1}{x_{10}^{N+1}}. \tag{A6}$$

$$x_{i+1} = 1 + (1-P_{local})P_{local}^r x_i^{r+1}, \tag{A7}$$

where $x_0 = 1$. r denotes the number of consecutive correct predictions. Therefore, the min-entropy can be derived from the following equation:

$$H_{min} = -log_2(max(P_{global}, P_{local})). \tag{A8}$$

Appendix B Optimization process

We present the effects of four structure parameters,which are: virtual node count, injection strength, feedback strength, and frequency detuning.

Appendix B.1 Relative error

In this paper, we select the normal distribution rounded to integers to train the PRC system model. Its theoretical min-entropy is calculated to be 6.2039. We select 0.8 M samples for training and 0.2 M samples for testing. In order to quantify the results of the min-entropy evaluation, we introduce the relative error, which is calculated as follows [8, 9]:

$$Relative\ error = \frac{\left|H_{min} - \hat{H}_{min}\right|}{H_{min}} \times 100\%, \tag{B1}$$

where H_{min} is the theoretical min-entropy and $\hat{H}_{min}$ is the evaluation result.

Appendix B.2 Effect of the structure parameters

Figure B1 shows the effect of the number of virtual nodes N. The number of virtual nodes can be adjusted by altering the node interval θ. When optimizing the number of virtual nodes N in PRC, we set other structure parameters as follows: injection strength $k_{inj} = 0.15$, feedback strength $k_f = 0.1$ and frequency detuning $\Delta\nu = 5$ GHz. Under these parameter configurations, the PRC system operates at the edge of the chaos region, exhibiting dual characteristics of nonlinearity and dynamic stability. These two characteristics can provide better prediction performance of PRC. As shown in the figure, the relative error initially decreases and then stabilizes as N increases. A smaller number of virtual nodes makes it difficult to map the input signal to a higher dimensional space. As the number of virtual nodes increases, the dimension of the state space also increases. However, a high number of virtual nodes can slow down the training process. Therefore, the number of virtual nodes N is fixed to 5000, where the relative error is 0.0796.

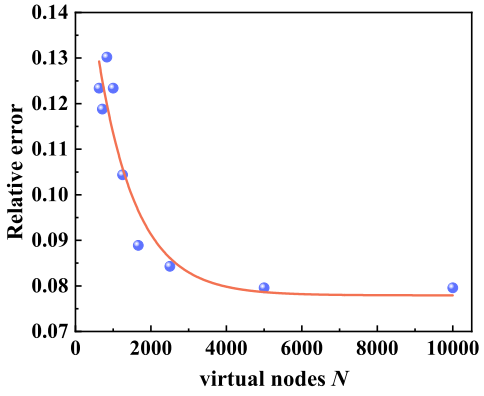

Figure B1 Effect of the number of virtual nodes N on the PRC performance.

After optimizing and fixing the number of virtual nodes N in PRC, we first investigate the effect of injection strength k_{inj}. Figure B2(a) shows the relationship between the injection strength k_{inj} and the relative error. Here, the feedback strength k_f and frequency detuning $\Delta\nu$ are set to 0.1 and 5 GHz, respectively. It can be seen that the relative error initially decreases as the injection strength k_{inj} increases and then stabilizes after 0.05. The smallest relative error, 0.0796, is observed at an injection strength of 0.3. Figure B2(b) presents the bifurcation diagram of the R-L output as a function of injection strength. It can be observed that output state of the R-L is in the injection-locked state when the injection strength is 0.3. In this state, the system can maintain optimal consistency, which is one of the key characteristics that PRC must satisfy [11, 12].

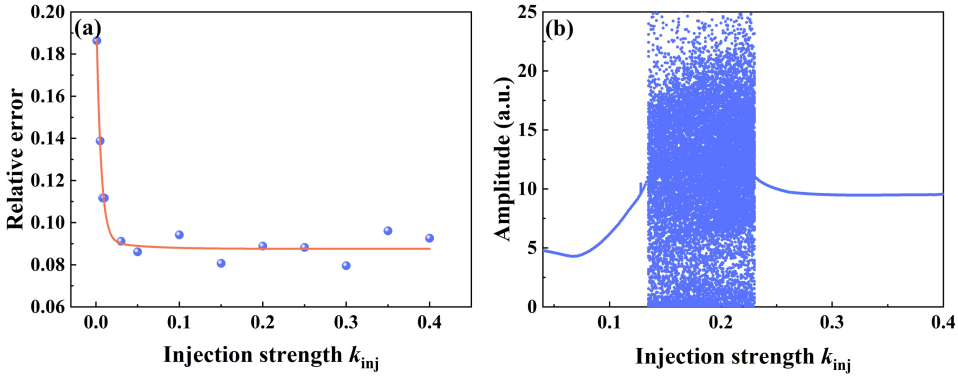

Figure B2 (a) Relative error versus the injection strength k_{inj} for $k_f = 0.1$ and $\Delta\nu = 5$ GHz. (b)Bifurcation diagram of the R-L output with increasing of the injection strength.

Figure B3(a) examines the effect of the feedback strength k_f. Here, the injection strength k_{inj} and frequency detuning $\Delta\nu$ are set to 0.3 and 5 GHz, respectively. As the feedback strength k_f increases, the relative error decreases at first, reaching a minimum value of 0.0664 at $k_f = 0.1$. By continuing to increase the feedback strength k_f, the relative error gradually increases again. This is because as the feedback strength k_f increases, R-L gradually enters a chaotic state. From the bifurcation diagram shown in Figure B3(b), it can also be seen that as the feedback strength increases, the output state of R-L gradually transitions from a steady state to a chaotic state. During this process, the system becomes more sensitive to changes in initial conditions, making it unable to maintain good short-term memory, which leads to a decline in PRC performance [12].

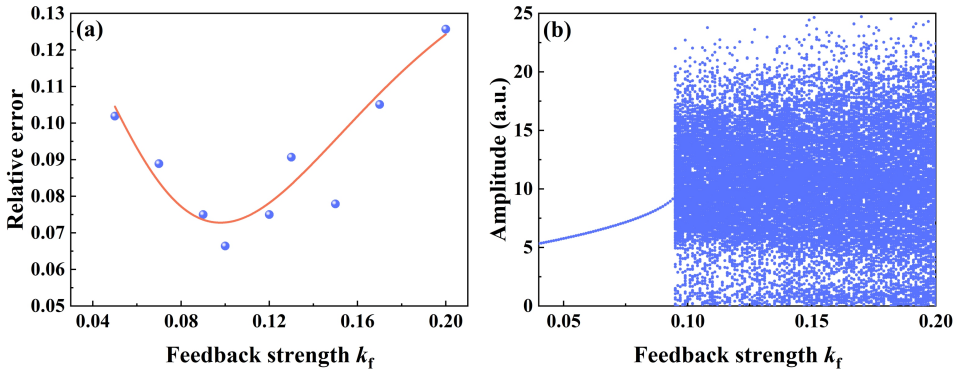

Figure B3 (a) Relative error versus the feedback strength k_f for $k_{inj} = 0.3$ and $\Delta\nu = 5$ GHz. (b) Bifurcation diagram of the R-L output with increasing of the feedback strength.

Finally, we discuss the effect of the frequency detuning $\Delta\nu$, as shown in Figure B4. Here, the injection strength k_{inj} and feedback strength k_f are set to 0.3 and 0.1, respectively. Figure B4(a) illustrates the relationship between frequency detuning $\Delta\nu$ and relative error. The relative error initially decreases and then increases as the frequency detuning $\Delta\nu$ increases. The relative error reaches a minimum of 0.0573 at $\Delta\nu = -5$ GHz. Figure B4(b) presents the bifurcation diagram as a function of frequency detuning $\Delta\nu$. From the bifurcation diagram, it can be seen that the R-L is at the edge of the chaotic region when $\Delta\nu = -5$ GHz, at which point the PRC provides good non-linearity.

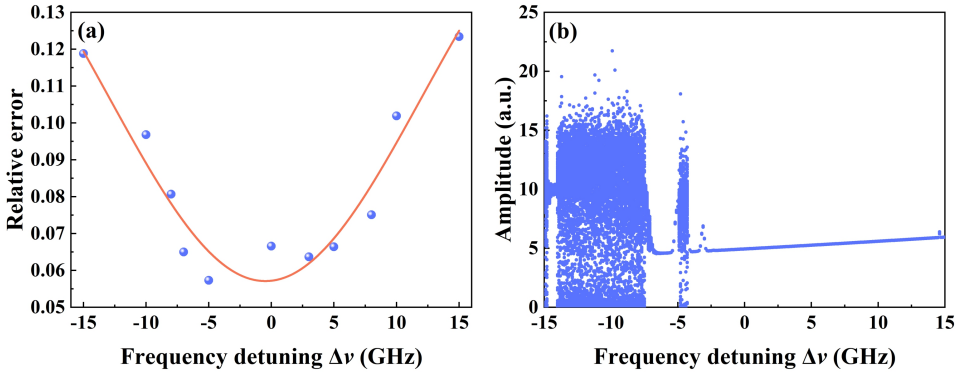

Figure B4 (a) Relative error versus the frequency detuning $\Delta\nu$ for $k_{inj} = 0.3$ and $k_f = 0.1$. (b) Bifurcation diagram of the R-L output with increasing of the frequency detuning.

Appendix C Evaluation results and analysis

After training the PRC structure parameters by simulating the source with a normal distribution, we evaluate 40 sets of data with several other distributions, quantized into different bits.

Figure C1(a) describes the evaluation results for the simulated sources with uniform distributions. It can be seen that PRC provides accurate evaluation results, which coincide with the theoretical min-entropy. However, NIST SP 800-90B underestimates the min-entropy of the entropy source at higher bits, possibly due to overfitting. Figure C1(b) shows the evaluation results for near-uniform distributions. Both PRC and NIST SP 800-90B provide more accurate evaluations. Their results at lower bits align with the theoretical min-entropy, while they are overestimated at higher bits. Figure C1(c) shows the evaluation results for normal distributions. From the figure, it can be seen that NIST SP 800-90B grossly underestimates the min-entropy of the entropy source. The results of the PRC evaluation, although also biased, are more accurate compared to those of NIST SP 800-90B.

Subsequently, we calculate the mean relative error between the lowest NIST SP 800-90B evaluation value and the PRC evaluation value for 40 sequences from each class of simulated sources to quantify the evaluation results, as a way to compare the evaluation performance of the two models. The mean relative error is the average of the relative errors of the min-entropy evaluation results for 40 sequences generated from each class of entropy source. As shown in Table C1, the mean relative error of the PRC evaluation results is lower than that of NIST SP 800-90B for all three types of simulated sources evaluated.

We further evaluate the min-entropy of the M-sequence to compare the performance of NIST SP 800-90B and PRC. The theoretical min-entropy of a periodic sequence is 0. As shown in Table C2, PRC provides completely accurate evaluation results at lower stages. Although the results become biased at higher stages, they are still better compared to all four predictors of NIST SP 800-90B.

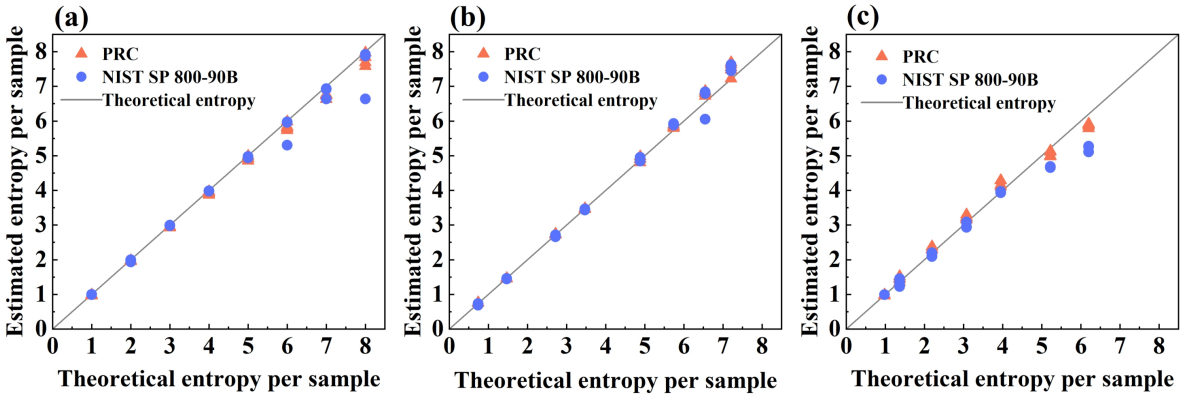

Figure C1 Comparison of the PRC and NIST SP 800-90B evaluation results for (a) uniform distributions, (b) near-uniform distributions, and (c) normal distributions.

Table C1 Mean relative error of different predictors estimations results.

Simulated data sets	NIST SP 800-90B (%)	PRC (%)
Uniform	2.70	2.49
Near-uniform	2.36	2.23
Normal	4.94	4.06

Table C2 Estimated results for M-sequence (theoretical min-entropy $H_{min} = 0.000$).

Stage	8	10	12	14	16	18
MultiMCW	0.991	0.996	0.988	0.989	0.993	0.999
Lag	1.000	1.000	1.000	1.000	1.000	1.000
MultiMMC	0.000	0.000	0.000	0.000	0.000	1.000
LZ78Y	0.991	0.994	0.997	0.996	0.996	0.997
PRC	0.000	0.000	0.000	0.000	0.000	0.891

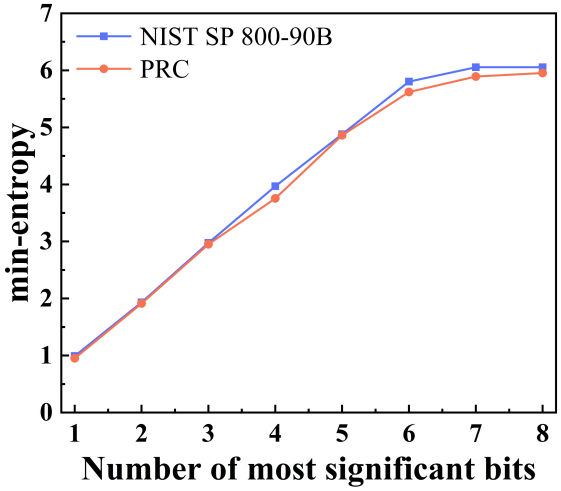

Figure C2 Min-entropy of the PRC predictor and NIST SP 800-90B predictor for n MSBs of white chaos.

To further validate the performance of the PRC method in min-entropy evaluation, we applied it to TRNGs. As shown in Figure C2, we evaluate the min-entropy of the white chaos by retaining n ($n = 1, 2, \ldots, 8$) MSBs. It can be seen that the min-entropy increases monotonically with the number of retained MSBs, and PRC yields a lower entropy evaluation value than NIST SP 800-90B.

References

1 Truong N D, Haw J Y, Assad S M, et al. Machine learning cryptanalysis of a quantum random number generator. IEEE Trans Inf Forensics Security, 2019, 14: 403-414.

2 Kelsey J, McKay K A, Turan M S. Predictive models for min-entropy estimation. In: 17th International Workshop on Cryptographic Hardware and Embedded Systems, 2015, 9293: 373-392.
3 Wang A B, Wang L S, Li P, et al. Minimal-post-processing 320-Gbps true random bit generation using physical white chaos. Opt Express, 2018, 25: 3153-3164.
4 Guo Y, Cai Q, Li p, et al. Ultrafast and real-time physical random bit extraction with all-optical quantization. Adv. Photonics, 2022, 4: 035001.
5 Lang R, Kobayashi K. External optical feedback effects on semiconductor injection laser properties. IEEE J Quantum Electron, 1980, 16: 347-355
6 Jiang N, Wang Y J, Zhao A K, et al. Simultaneous bandwidth-enhanced and time delay signature-suppressed chaos generation in semiconductor laser subject to feedback from parallel coupling ring resonators. Opt Express, 2020, 28: 1999-2009
7 Heil T, Fischer I, Elsasser W, et al. Chaos synchronization and spontaneous symmetry-breaking in symmetrically delay-coupled semiconductor lasers. Phys Rev Lett, 2001, 86, 795-8.
8 Turan M S, Barker E, Kelsey J, et al. NIST special publication 800-90B: recommendation for the entropy sources used for random bit generation. National Institute of Standards and Technology, 2018.
9 Li H H, Zhang J G, Li Z H, et al. Improvement of min-entropy evaluation based on pruning and quantized deep neural network. IEEE Trans Inf Forensics Secur, 2023, 18: 1410-1420.
10 Huang Y L, Fan F, Huang C F, et al. MA-DG: Learning features of sequences in different dimensions for min-entropy evaluation via 2D-CNN and multi-head self-attention. IEEE Trans Inf Forensics Secur, 2024, 19: 7879-7894.
11 Kai C, Li P, Yang Y, et al. Forecasting the chaotic dynamics of external cavity. Opt Lett, 2023, 48: 1236-1239. semiconductor lasers.
12 Li J Y, Cai Q, Li P, et al. Image recognition based on optical reservoir computing. Chaos, 2022, 32: 123106.