SCIENCE CHINA
Information Sciences

• LETTER •

August 2025, Vol. 68, Iss. 8, 189402:1–189402:2
https://doi.org/10.1007/s11432-025-4382-4

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 of China, 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*

Received 1 February 2025/Revised 31 March 2025/Accepted 14 April 2025/Published online 1 July 2025

Citation Wang J J, Cai Q, Zhang J G, et al. Photonic reservoir computing based min-entropy evaluation for random number generators. Sci China Inf Sci, 2025, 68(8): 189402, https://doi.org/10.1007/s11432-025-4382-4

Random numbers are fundamental to cryptography and secure communications. Random number generators (RNGs) are usually classified into pseudo random number generators and true random number generators. If the outputs of RNGs are not sufficiently secure, they become vulnerable to unauthorized access, exposing cryptographic systems to significant security risks [1]. Ensuring the security of RNGs is significantly critical, requiring extensive testing and evaluation to validate their reliability.

There are two primary methods for evaluating the security of RNGs: white-box testing and black-box testing. White-box testing involves mathematically modeling the entropy source to calculate the entropy of the output sequences, but this process is complex. Black-box testing is further divided into statistic-based and prediction-based methods. Statistic-based approaches use standard test suites to evaluate the security of random numbers. However, these can sometimes fail to distinguish pseudo-random sequences with strong statistical properties, making reliance on statistical test suites alone insufficient.

Prediction-based methods have emerged in recent years, leveraging neural networks to evaluate RNG security. Among these, min-entropy is a commonly used metric in neural networks for assessing the security of entropy sources [2]. Defined in the National Institute of Standards and Technology Special Publication (NIST SP 800-90B), it serves as a conservative quantification of min-entropy [3]. However, the traditional process of training neural network models remains complex, computationally expensive, and challenging to implement in hardware owing to structural limitations.

Reservoir computing is recognized as a promising alternative. This novel artificial neural network framework requires only the training of output layer weights using a simple learning algorithm, which makes it highly computationally efficient [4]. Furthermore, photonic reservoir computing (PRC), based on semiconductor lasers with time-delayed feedback, features a single nonlinear physical node. This architecture enables higher data injection rates [5] and has proven effective in applications such as chaotic time-series prediction, speech and image recognition, and nonlinear channel equalization. Therefore, applying PRC to evaluate min-entropy holds great promise.

This study proposes a novel approach using single node-based PRC to evaluate min-entropy for RNGs. PRC predicts future outputs by identifying the hidden relationships within random number sequences and calculates min-entropy based on the probability of correct predictions. Its design, which involves a simple structure with a nonlinear physical node, reduces overall system complexity and makes it suitable for hardware implementation while maintaining high computational efficiency. To the best of our knowledge, our proposed method is the first to use PRC for evaluating min-entropy, thus expanding its application in the field of random numbers. Additionally, the results of this approach outperform NIST SP 800-90B, providing a more conservative evaluation of RNG security.

Theoretical model of PRC. Figure 1 illustrates the PRC system for min-entropy evaluation. This system is designed using a semiconductor laser with self-delayed feedback and consists of an input layer, a reservoir layer, and an output layer. To effectively train the PRC model for evaluating the min-entropy of random numbers, the input data undergoes

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

preprocessing. In our scheme, the preprocessing process is as follows. Ten consecutive samples of random numbers are selected as inputs, with the subsequent sample designated as the target value. The data are then shifted backward by 3 samples. The next ten shifted samples serve as the new input sequence, while the eleventh shifted sample becomes the target value for model training. This process is repeated iteratively to generate input sequences and corresponding target values. In this study, we use five types of random number simulated datasets as input data. Four of these datasets have known theoretical min-entropy values, indicating discrete uniform distribution, discrete near-uniform distribution, normal distribution rounded to integers, and M-sequence. The fifth dataset represents a true random number sequence derived from white chaos. The details of the datasets are provided in Appendix A.

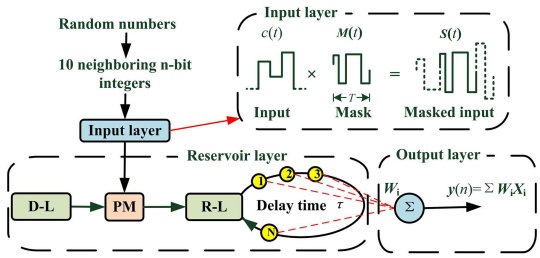

Figure 1 (Color online) Schematic diagram of PRC. D-L: drive laser. R-L: response laser. PM: phase modulator.

In the input layer, the input sequence $c(t)$ in Figure 1 is derived from the preprocessing stage. Each data point in the sequence is sampled and held for a period of T, corresponding to the feedback delay time. This sequence is then multiplied by a mask signal $\boldsymbol{M}(t)$, also with a period of T, to obtain $\boldsymbol{S}(t)$. Here the mask comprises random-level signal $\{-1, 1\}$. The sequence $\boldsymbol{S}(t)$ is loaded onto the output light of the drive laser (D-L) by phase modulation and then injected into the response laser (R-L). The feedback delay time of the R-L, defined as τ, plays a key role in the reservoir layer. The outputs of the R-L are sampled at equal intervals with a sampling interval of θ, yielding N virtual node states, where $N = \tau/\theta$. In our work, the feedback delay time τ is 50 ns. A simulation model of the PRC is provided in Appendix A.

In the output layer, the PRC output $\boldsymbol{y}(n)$ corresponding to the n-th input data is computed as a linear combination of the output connection weights $\boldsymbol{W}_i$ and the virtual nodes $\boldsymbol{X}_i$, defined as

$$\boldsymbol{y}(n) = \Sigma \boldsymbol{W}_i \boldsymbol{X}_i. \tag{1}$$

In our work, the ridge regression algorithm is used to train the output weights.

The probability of correct prediction is calculated based on the PRC output, yielding the global predictability P_{global} and local predictability P_{local}. Finally, the min-entropy is calculated using

$$H_{\min} = -\log_2(\max(P_{\text{global}}, P_{\text{local}})). \tag{2}$$

Further details on the min-entropy calculation process are provided in Appendix A.

Structure parameters optimization of PRC. The structural parameters of PRC significantly affect system performance. We sequentially optimized four structure parameters: the number of virtual nodes N, the injection strength k_{inj}, the feedback strength k_f, and the frequency detuning $\Delta\nu$. The final optimal structure parameters are determined as follows: the number of virtual nodes $N = 5000$, $k_{inj} = 0.3$, $k_f = 0.1$, and $\Delta\nu = -5$ GHz. Further details on the optimization process are provided in Appendix B.

Evaluation results. After optimizing the PRC structure parameters to their optimal values, we use PRC for min-entropy evaluation. For the first three types of data sources, the mean relative error from 40 sequences improved accuracy compared to NIST SP 800-90B. For the M-sequence, the PRC provided entirely accurate results for stages below 16. For the white chaos true random number sequence, the entropy evaluation from PRC was more conservative than that of NIST SP 800-90B, offering a more conservative assessment. Detailed results are presented in Appendix C.

Conclusion. We present a novel method for evaluating the min-entropy of random number generators using PRC. By investigating the effects of PRC structural parameters on performance, we identified the optimal parameter settings. To validate the accuracy of this method, evaluations were conducted using various simulated data sources with theoretical min-entropy values derived from their own probability distributions. The results prove that our PRC model achieves performance on par or superior to that of the NIST SP 800-90B standard. Furthermore, for true random numbers with unknown min-entropy, our PRC model produces a lower min-entropy value than that of the NIST SP 800-90B standard. Consequently, our proposed PRC model represents a robust and reliable tool for entropy evaluation.

Acknowledgements This work was supported in part by National Key Research and Development Program of China (Grant No. 2024YFB2808400), National Natural Science Foundation of China (Grant Nos. 62175177, 62322504), Guangdong Introducing Innovative and Entrepreneurial Teams of The Pearl River Talent Recruitment Program (Grant No. 2019ZT08X340), and Fundamental Research Program of Shanxi Province (Grant No. 202403021222277).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Li H, Zhang J, Li Z, et al. Improvement of min-entropy evaluation based on pruning and quantized deep neural network. IEEE Trans Inform Forensic Secur, 2023, 18: 1410–1420
2 Huang Y, Fan F, Huang C, 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 Inform Forensic Secur, 2024, 19: 7879–7894
3 Turan M S, Barker E, Kelsey J, et al. Recommendation for the Entropy Sources Used for Random Bit Generation: NIST SP 800-90b. North Charleston: CreateSpace Independent Publishing Platform, 2018
4 Appeltant L, Soriano M C, van der Sande G, et al. Information processing using a single dynamical node as complex system. Nat Commun, 2011, 2: 468
5 Brunner D, Soriano M C, Mirasso C R, et al. Parallel photonic information processing at gigabyte per second data rates using transient states. Nat Commun, 2013, 4: 1364