


Article

Key Space Enhanced Correlated Random Bit Generation Based on Synchronized Electro-Optic Self-Feedback Loops with Mach–Zehnder Modulators

Chuyun Huang ¹ , Xulin Gao ¹, Sile Wu ¹, Wenfu Gu ¹, Biao Su ¹, Yuncai Wang ^{1,2}, Yuwen Qin ¹ and Zhensen Gao ^{1,2,*}

¹ Institute of Advanced Photonics Technology, School of Information Engineering, Guangdong Provincial Key Laboratory of Photonics Information Technology, Guangdong University of Technology, Guangzhou 510006, China

² Pengcheng Laboratory, Shenzhen 518052, China

* Correspondence: gaozhensen@gdut.edu.cn

Abstract: With the widespread application of big data, the amount of data transmitted through optical networks has been increasing dramatically. Correlated random bit generation (CRBG) is one of the key technologies in secure communication systems to ensure security performance and transmission efficiency. We propose and demonstrate a CRBG scheme based on a Mach–Zehnder modulator (MZM) electro-optic feedback loop to improve the security and speed of communication systems. In this scheme, common-signal-induced synchronization is accomplished to generate wideband complex physical entropy sources, and a private hardware module is employed to perform post-processing and nonlinear transformation of the synchronized signal. The simulation results show that the effective bandwidth of the output chaotic signal is significantly increased to 27.76 GHz, and high-quality synchronization with a correlation coefficient of over 0.98 is reached. A high-rate CRBG of up to 5.3 Gb/s is successfully achieved between two synchronized wideband physical entropy sources, and the hardware key space is enhanced to $\sim 2^{42}$, which greatly improves the privacy of physical entropy sources. The proposed scheme provides a promising approach for high-speed private CRBG, which is expected to be used in high-speed secure key distribution and optical communication systems.

Keywords: correlated random bit generation; physical entropy source; nonlinear transformation; key space



Citation: Huang, C.; Gao, X.; Wu, S.; Gu, W.; Su, B.; Wang, Y.; Qin, Y.; Gao, Z. Key Space Enhanced Correlated Random Bit Generation Based on Synchronized Electro-Optic Self-Feedback Loops with Mach–Zehnder Modulators. *Photonics* **2022**, *9*, 952. <https://doi.org/10.3390/photonics9120952>

Received: 10 November 2022

Accepted: 6 December 2022

Published: 9 December 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Random numbers are widely used in information security schemes as passwords and keys to ensure the confidentiality, integrity, and authenticity of communications [1]. The key system needs to generate truly correlated random bits to ensure that the detection parameters are unpredictable. Generators of random numbers can be classified into two categories: pseudorandom number generators and physical random number generators. The pseudorandom number is generated by the deterministic algorithm, and it will remain in the same sequence if the generation seed is unchanged, which will bring serious problems to the information security system.

Physical random number generators provide non-deterministic random bits by measuring unpredictable physical processes, thus ensuring privacy, such as in the frequency jitter of oscillators [2], thermal noise from resistors [3], electrical chaos in nonlinear circuits [4], and photon events in attenuated light [5]. However, these traditional physical random number generators are limited in bandwidth and restrained at a slow rate (Mbps), which is insufficient to meet the requirements of modern secure communications with data rates of Gbps. Therefore, wide-bandwidth high-speed correlated random bit generation (CRBG) on both sides is the key point to break through for secure communication.

In recent years, many researchers have been devoted to improving the speed of physical random bit generators for the requirement of modern secure communications. Laser chaos [6–14], amplified spontaneous emissions [15], quantum vacuum states [16,17] and laser phase noise [18] are widely used as physical entropy sources for generating Gbps and even faster non-deterministic random bits [19]. Electro-optical chaos [20] is another very attractive physical entropy source that can generate high-speed random numbers due to its large bandwidth. However, it is highly desirable to generate synchronized random numbers for secure key distribution, so CRBG is getting more attention. The generation of correlated random bits through the synchronization of two physical entropy sources has also been studied extensively [9–13,21–23]. Kanter et al. numerically verified a CRBG scheme at a speed of over Gbps using synchronization between two bidirectionally coupled chaotic lasers [10]. Shao et al. also realized ~ 1.25 Gb/s CRBG based on an electro-optical chaotic entropy source [11]. Wang et al. demonstrated ~ 2.5 Gb/s CRBG using synchronous chaos induced by common lasers with dispersion feedback [24]. Fabian Böhm et al. proposed a method based on an optoelectronic oscillator that successfully implemented synchronized random bits at a rate of 6 Gb/s [25]. Recently, we also experimentally realized CRBG recordings of up to 5.2 Gb/s with synchronized wideband physical entropy sources based on hybrid electro-optic nonlinear transformation [22]. However, the security of these systems needs to be improved because the hardware variable parameters are notably insufficient, which limits the key space. In addition, the limited bandwidth of several gigahertz for traditional physical entropy sources, such as a laser chaotic source, greatly limits the CRBG rate [26].

Although a lot of work has been done to extract high-speed correlated random bits from various wideband physical entropy sources, high-speed CRBG is not an easy task due to the difficulty of achieving high-quality synchronization of wideband signals [23]. In this work, we propose and demonstrate a high-speed and private CRBG scheme that modulates chaotic signals into the phase variation of the light using a phase modulator (PM) and finally expands the chaotic bandwidth with the participation of dispersion structures while ensuring chaotic synchronization. We further use an electro-optical self-feedback loop based on a Mach–Zehnder modulator (MZM) to improve the key space and further expand the chaotic bandwidth. The results show that the synchronized wideband physical entropy sources successfully achieve a high-quality synchronization of over ~ 0.98 and a low correlation level of ~ 0.059 between the drive and response signals. The bandwidth expansion of the synchronized wideband physical entropy source is more than double, the CRBG rate is up to 5.3 Gb/s, and $\sim 2^{42}$ hardware key space is enhanced, which greatly improves the privacy of the physical entropy sources. Correlated random bit sequences (CRBSs) could successfully be proved to have good randomness by relying on industry-standard benchmark tests provided by the National Institute of Standards and Technology (NIST) [27].

2. Principle of CRBG Setup

Figure 1 illustrates the principle and simulation setup of the proposed high-speed private CRBG scheme. In the proposed scheme, a chaotic signal with an optical feedback is used as the common drive signal with limited initial chaos bandwidth and low complexity. Then, under the effect of spectrum spreading caused by the phase modulation (PM) and phase-modulation-to-intensity-modulation (PM-to-IM) conversion of a dispersion component, synchronized wideband physical entropy sources are obtained through the electro-optical self-feedback amplitude modulation loop based on an MZM. On this basis, two synchronous wideband physical entropy sources are accomplished to obtain high-rate CRBGs.

Specifically, a distributed feedback (DFB) laser with an external fiber mirror feedback is used as the driving source of physical entropy to generate a random chaotic source signal $E_c(t)$. The bias current that drives the semiconductor laser (DSL) is 1.2 times the threshold current, and its wavelength is set to 1550 nm. The output common random chaotic source

The field transfer function of MZM is defined as:

$$h(t) = Ce^{j\omega} [e^{j(\frac{\pi V_{RF}}{V_{\pi}} + \frac{\pi V_{DC}}{V_{\pi}})} + e^{-j(\frac{\pi V_{RF}}{V_{\pi}} + \frac{\pi V_{DC}}{V_{\pi}})}] = \pm 2Ce^{j\omega}, \quad (4)$$

where C is a constant, V_{π} refers to the half-wave voltage of MZM, V_{RF} stands for the RF voltage, and V_{DC} is the DC bias voltage.

The RF voltage of MZM can be obtained by:

$$V_{RF} = \rho g S |E_0(t - \tau)|^2 - \delta \frac{dV_{RF}}{dt} - \frac{1}{\mu} \int_0^t V(\varepsilon) d\varepsilon, \quad (5)$$

where δ and μ are the characteristics response times of the band-pass filter, which is composed of AMP and PD. S denotes the sensitivity of PD, ρ denotes the optical power loss, g denotes the gain of AMP, and τ is the delay time.

The detailed key hardware parameters and the corresponding values in the scheme are illustrated in Table 1. Compared with traditional CRBG schemes, the proposed scheme contains more hardware parameters, such as phase modulation depth, the bidirectional delay time of the electro-optic self-feedback loop, DC bias voltage and the feedback depth of the MZM, and the dispersion value, which can greatly enhance the hardware key space and privacy of the CRBG. When the hardware parameters between Alice and Bob are well matched, the private CRBG can achieve high-quality synchronization.

Table 1. Values of parameters used in the simulation system.

Parameter	Description	Value
f	Center frequency of DSL	193.1 THz
L	Length of SMF	25 km
M_1	Modulation depth of PM_1	2.8
M_2	Modulation depth of PM_2	2.7
F_1	Feedback intensity of MZM_1	1.2
F_2	Feedback intensity of MZM_2	1.2
τ_1	Feedback time delay of Alice	3.03 ns
τ_2	Feedback time delay of Bob	3.03 ns
D_1	Dispersion of $CFBG_1$	400 ps/nm
D_2	Dispersion of $CFBG_2$	400 ps/nm
BW_1	Bandwidth of PD	40 GHz
BW_2	Bandwidth of MZM	40 GHz
I	Insertion loss of MZM	6 dB
R	Extinction ratio of MZM	35 dB

3. Results

3.1. Synchronization Characteristics of Chaos

Figure 2 shows the measured time waveforms generated by the common driving source and the synchronized wideband physical entropy sources, as well as the correlation between them. Figure 2a–c shows the signal waveforms of the driving chaotic source and the time waveforms of the output of the wideband physical entropy sources at Alice and Bob (respectively measured at positions A, C and D in Figure 1). Figure 2d shows the corresponding residual correlation between the chaotic source signal waveform and the time waveform output of the broadband physical entropy source at the Alice end. For phase-intensity hybrid modulation, the final response output waveform is completely different from the intensity fluctuation of the driving signal.

Compared with the traditional chaotic driving-response configuration, the residual correlation coefficient was significantly reduced to 0.059 using this scheme, while the value in the traditional scheme is usually much higher, up to 0.7 [28]. We further verified the waveform and found that the time delay signature (TDS) of common driving source is concealed. This indicates that there is no correlation information of random bits in the

public link, which enhances the privacy of the final output response signal. In addition, it is obvious that the time waveforms of Alice and Bob's two synchronized wideband physical entropy sources at C and D present almost the same profile, as shown in Figure 2b,c,e, and achieve a high correlation value of 0.986, indicating that CRBG based on this scheme can achieve high-quality synchronization.

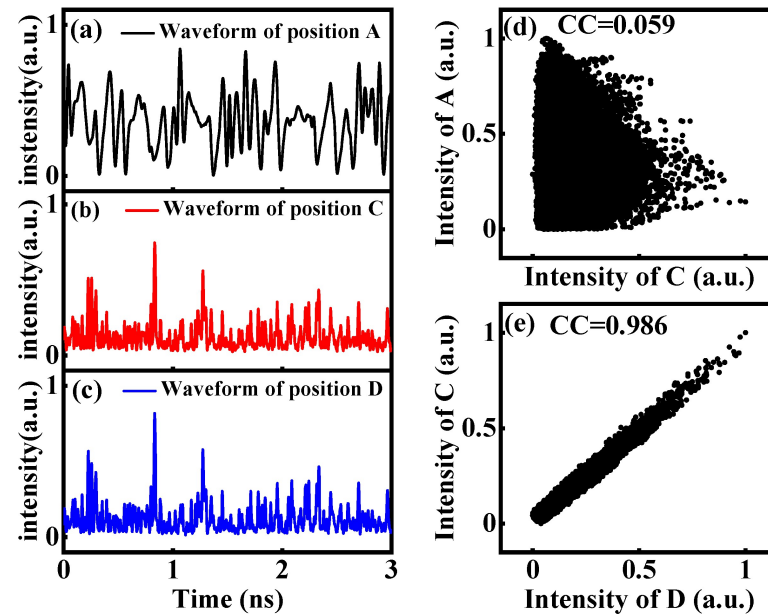


Figure 2. Temporal waveforms and the corresponding correlation plots of the output chaos. (a–c) show the normalized temporal waveforms of position A, C and D. (d) shows correlation plots of position A and C. (e) shows correlation plots of position C and D.

The RF spectrum of chaotic output is measured at positions A and C, and the results are shown in Figure 3a,b. Limited by the relaxation oscillation frequency of the semiconductor laser, the effective bandwidth of the original chaos is only ~ 10.78 GHz, which is defined by the spectral width covering eighty percent of the energy distribution in the whole spectrum range [29,30]. In contrast, after bandwidth enhancement, the effective bandwidth of the output physical entropy source is greatly expanded to ~ 27.76 GHz, more than twice the original chaotic bandwidth, as shown in Figure 3b, which will be of great benefit to high-rate CRBG.

3.2. Selection of System Physical Parameters

Since the hardware system cannot be completely consistent, we analyze and study the effects of system detuning, as shown in Figures 4–6, including MZM, PM, dispersion, etc. If the synchronization is lower than 0.9, the bit error rate of CRBG will be greatly increased, resulting in a lower key distribution rate and worse security performance. Therefore, 0.9 is used as the benchmark to determine the detuning range of variable hardware parameters in this system. The contour plots shown in Figure 4a–c demonstrate the cross-correlation between the output of the physical entropy sources at positions C and D when Alice and Bob's PM modulation depth, DC bias, and MZM feedback intensity vary, respectively.

It can be easily seen from Figure 4a that the modulation depth of the driving signal needs to be kept above 0.5. When the modulation depth of PM_1 and PM_2 is greater than 0.5, moreover, kept at the same degree, the chaos synchronization quality will be maintained at a high level. However, when the PM modulation depth is different, the output cross-correlation will decrease correspondingly, and become more obvious as the detuning degree increases.

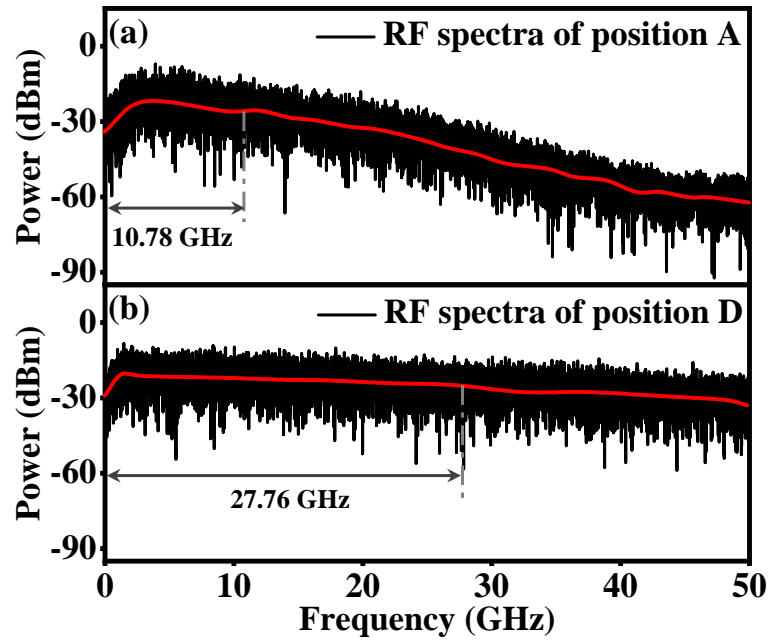


Figure 3. Measured RF spectra at (a) position A and (b) position D .

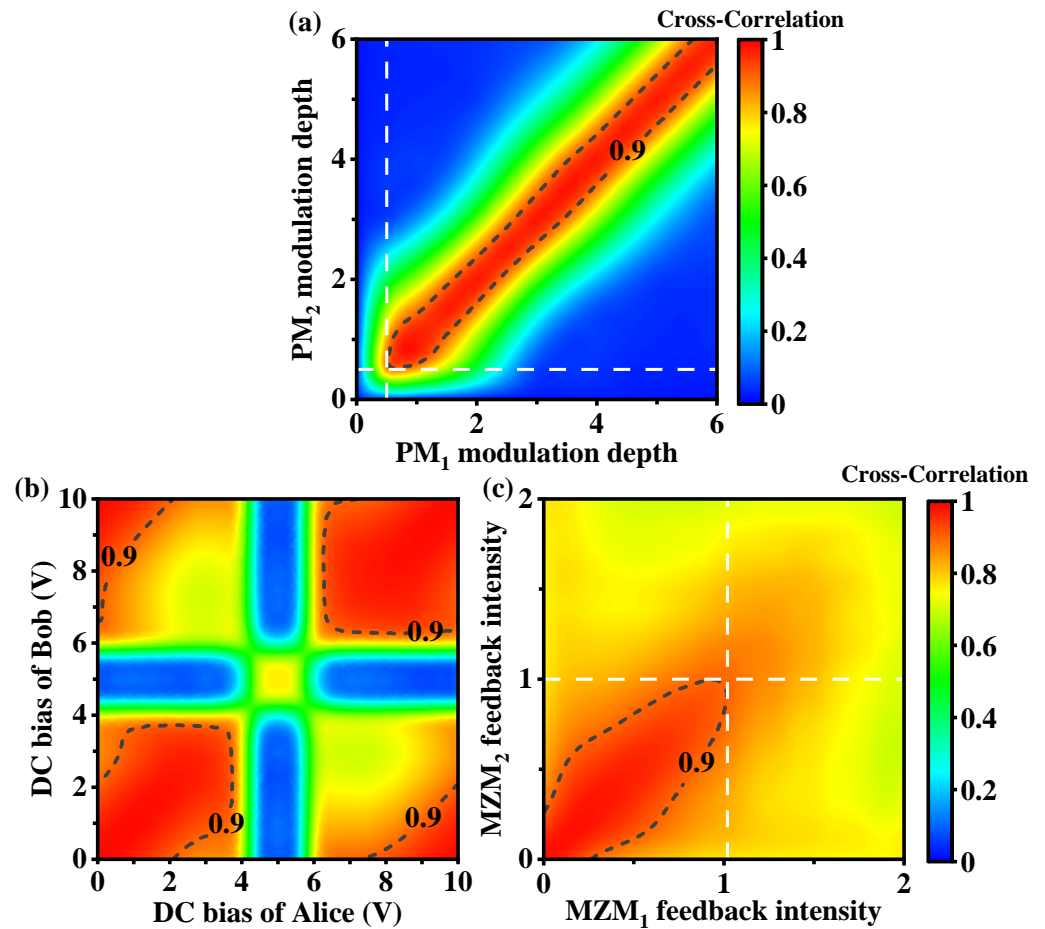


Figure 4. (a) Cross-correlation versus modulation depth of PM_1 and PM_2 ; (b) cross-correlation versus DC bias of Alice and Bob; (c) cross-correlation versus feedback intensity of MZM_1 and MZM_2 .

The MZM DC half-wave voltage is set at 5 V to measure the influence of DC bias voltage detuning on the response output cross-correlation, as shown in Figure 4b. Obviously, it can be seen from the figure that, within a certain range, when the two DC bias voltages are the same, the chaos synchronization quality stays at a higher level. However, when the two DC bias voltages are around multiples of 5, the output cross-correlation plummets to 0 as the voltages approaches 5. This is because the modulation curve of MZM is a cosine-like curve. When the DC voltage is set at the half-wave voltage, the output is close to 0 when it is at the trough value.

When the MZM bias voltage is set to 8V, the influence of MZM feedback intensity detuning on chaotic output cross-correlation is shown in Figure 4c. From the figure, it is clear that the feedback strength of MZM needs to be maintained at 1. When the feedback strength is the same and less than one, the quality of chaos synchronization remains at a high level. However, when the two MZM feedback intensities are different, the output cross-correlation will decrease correspondingly and become more obvious as the degree of detuning increases.

To further verify the conclusion above and determine the system parameters more accurately, we also compare the joint influence of MZM feedback depth and PM modulation depth, as well as MZM DC bias voltage and feedback depth, on the synchronization of two wideband physical entropy sources, as shown in Figure 5a,b.

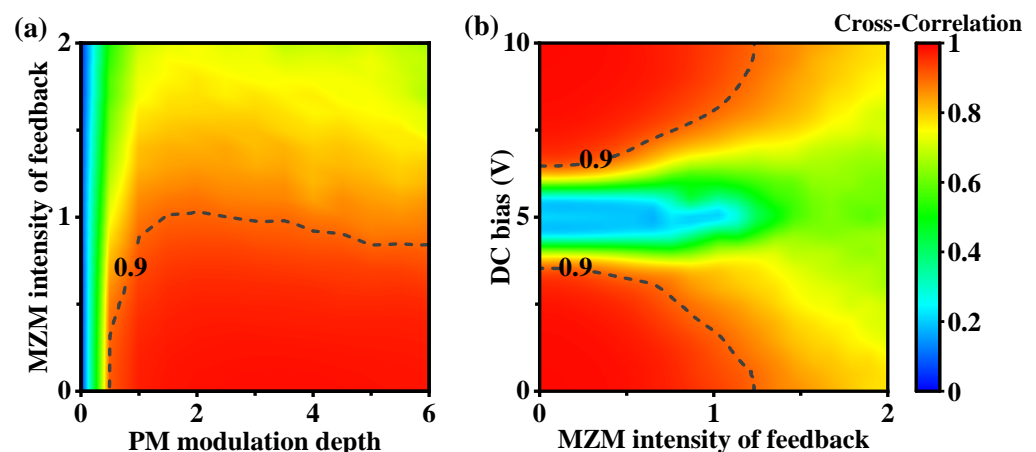


Figure 5. (a) Cross-correlation versus modulation depth of PM and feedback intensity of MZM; (b) cross-correlation versus DC bias and feedback intensity of MZM.

The influence of MZM feedback depth and PM modulation depth on the cross-correlation of Alice and Bob's output physical entropy sources is shown in Figure 5a. As can be seen from the figure, as the PM modulation depth increases, the output correlation increases. When the modulation depth is greater than 0.5, the output correlation is greater than 0.9. On the contrary, with the increase of MZM feedback strength, the output correlation will be lower. When the feedback strength is more than 1, the output correlation will be less than 0.9. Therefore, the modulation depth of the driving signal needs to be kept above 0.5, and the feedback strength of MZM needs to be lower than 1, which is consistent with the conclusion in Figure 4a,c.

As shown in Figure 5b, the DC bias voltage and MZM feedback strength of Alice and Bob are changed at the same time, and the relationship among DC bias voltage, MZM feedback strength and output cross-correlation is observed. The results show that when the feedback strength is less than ~ 1.23 , the output correlation is lower when the bias voltage is closer to the DC half-wave voltage of MZM, and the correlation is higher when the bias voltage is further away from the half-wave voltage. That is, the MZM feedback strength should be set within 1.23, and the DC bias voltage should be selected to avoid nearing multiples of 5.

In this scheme, a PM modulation depth of 3 times, MZM DC offset voltage of 8 V and MZM feedback depth of 0.2 are used for CRBG. The corresponding high cross-correlation value is ~ 0.986 , and the driving signal bandwidth and the synchronized wideband physical entropy sources bandwidth are ~ 10.78 GHz and ~ 27.76 GHz, respectively.

3.3. Tolerance of System Physical Parameters

After discussing the effects of PM modulation depth, MZM feedback depth, and DC bias on the synchronized wideband physical entropy sources, we now turn our attention to the exact tolerance of hardware parameter mismatch of wideband physical entropy sources. Figure 6 shows the relationship between the cross-correlation performance measured at C and D and key hardware parameter detuning, including (a) PM modulation depth detuning, (b) dispersion value detuning, (c) MZM feedback depth detuning, (d) MZM DC bias detuning and (e) self-feedback loop delay time detuning.

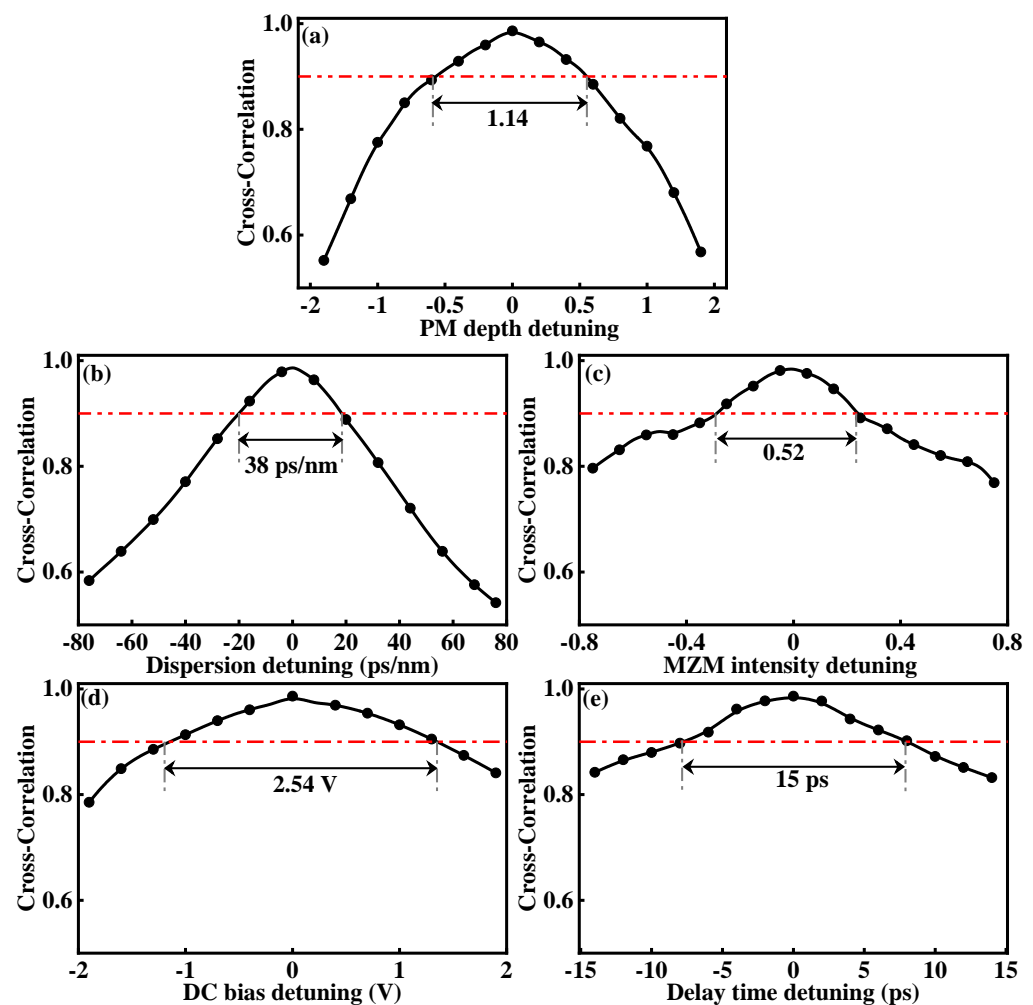


Figure 6. Cross-correlation between Alice and Bob versus (a) PM depth detuning, (b) dispersion detuning, (c) MZM intensity detuning, (d) DC bias detuning, and (e) delay time detuning.

The mismatch of these hardware key parameters of the physical entropy source between Alice and Bob will lead to a decrease in cross-correlations. The PM modulation depth mismatch tolerance is ~ 1.14 , the MZM feedback depth detuning is ~ 0.52 , the MZM DC bias detuning is ~ 2.54 V, the delay time is ~ 15 ps, the correlation number is reduced to ~ 0.9 , and the dispersion is ~ 38 ps/nm, which are all within the controllable range of commercial optical products. Therefore, the phase-intensity module is added to the synchronized wideband physical entropy sources. Based on the key space analysis in

reference [31], the hardware key space enhancement of $\sim 2^{42}$ is expected to be achieved by assuming the maximum value that each hardware parameter can reach in practice.

3.4. Estimation of Entropy Source Rate

To predict the maximum CRBG rate, the entropy source rate of optical chaos is first estimated. The entropy source rate is defined as the maximum generation rate of random bits verified by the single-bit quantization method [32,33] for randomness. The output signals of point B and point D are sampled at different sampling rates. Subsequently, the sampled signal is quantized into a binary sequence, where the quantization threshold is the median of the selected amplitude distribution to ensure that the quantization bits of “0” and “1” have equal probability while guaranteeing randomness, and a final test sequence is produced in the end.

The randomness of the test sequence was then examined by the National Institute of Standards and Technology Special Publication 800-22 Statistical Test (NIST SP800-22), which consists of 15 statistical test items. If all 15 items of NIST passed, the test sequence was considered to meet the randomness requirement. Figure 7a,b show the test results of B output chaotic and D point wideband physical entropy sources, respectively. The median number of items passed is indicated by a hexagon, and the maximum and the minimum number of items passed are indicated by red bars. As can be seen from the figure, in the output signal of point B, the maximum pass rate of CRBG is ~ 7.14 Gb/s, and the corresponding entropy source rate is ~ 7.14 Gb/s. The bandwidth expansion signal of the wideband physical entropy source at point D has an entropy source rate of up to ~ 25 Gb/s, which can greatly increase the CRBG rate.

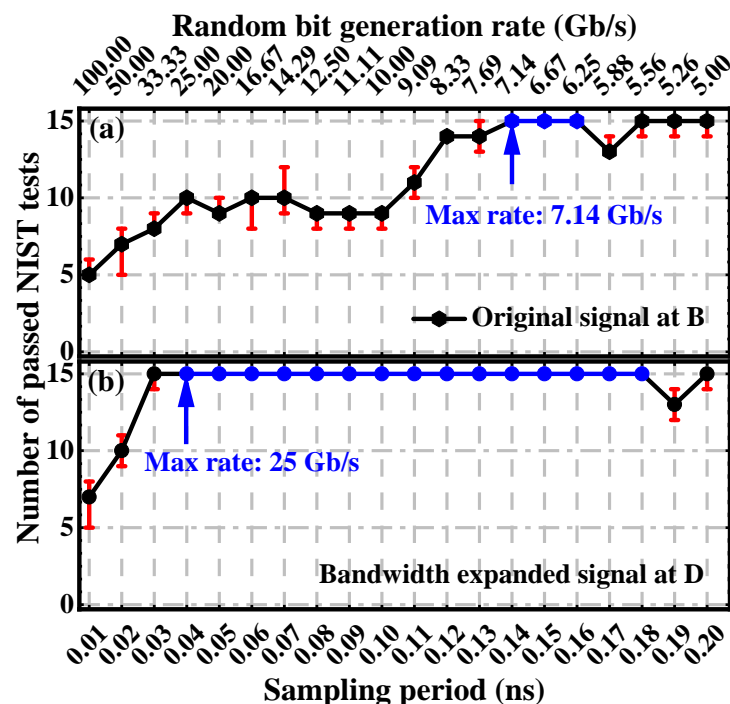


Figure 7. Entropy rate performance for (a) the original signal at B and (b) the bandwidth expanded signal at D.

Then, the entropy source rate of ~ 25 Gb/s is taken as the sampling rate, and the robust double threshold quantization method [34] is used to extract the CRBSs from the signal with bandwidth expansion. The threshold gap is defined as the difference between the high threshold and the low threshold, which is a key factor in double threshold quantization. Its influence on bit error rate and bit rate is shown in Figure 8. With an increase in the threshold gap, the bit error rate and bit rate decrease correspondingly due to the increase

in discarded noise-sensitive sampling points. When the normalized quantization threshold is greater than ~ 0.35 , the bit error threshold for hard-decision forward-error correction (HD-FEC) will be lower than 3.8×10^{-3} .

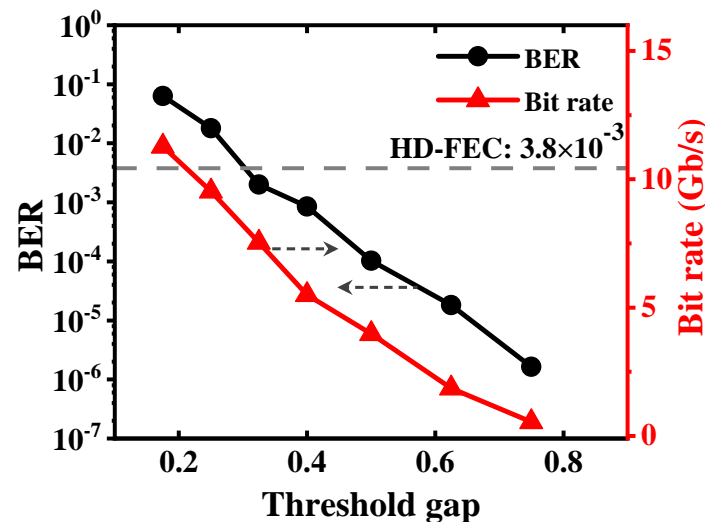


Figure 8. BER and bit rate versus threshold gap.

When the normalized quantization threshold is 0.35, the corresponding random bit retention rate is 0.213, the final CRBG rate is 5.3 Gb/s ($25 \text{ Gb/s} \times 0.213$), and the BER is lower than the HD-FEC threshold. This high-speed CRBG is a broadband physical entropy source based on phase modulation and dispersion to realize phase-to-intensity conversion combined with a hybrid electro-optic nonlinear transformation module.

Finally, we further verified the randomness of the final CRBG, and the test results of 50×10^6 -bit long keys for testing are shown in Table 2. As can be seen from the test report in the table, the P-values are all greater than 0.0001, and the proportions are within the confidence interval of 0.99 ± 0.0094392 [35], indicating that CRBG with a final rate of 5.3 Gb/s can pass all 15 NIST tests and meet the randomness requirements of CRBG.

Table 2. Randomness test results of the final obtained CRBG.

15 NIST Tests	P-Value	Proportion	Decision
Frequency	0.20953	98.3	Success
Block Frequency	0.87433	99.7	Success
Cumulative Sums	0.33427	98.6	Success
Runs	0.21352	99.0	Success
Longest Run	0.69613	98.5	Success
Rank	0.81684	99.8	Success
FFT	0.34325	98.1	Success
Non-Overlapping Template	0.67723	99.4	Success
Overlapping Template	0.95799	99.1	Success
Universal	0.50993	99.7	Success
Approximate Entropy	0.43752	98.2	Success
Random Excursions	0.93138	98.4	Success
Random Excursions Variant	0.71700	99.7	Success
Serial	0.62051	99.8	Success
Linear Complexity	0.74785	98.3	Success

4. Conclusions

In conclusion, we propose and demonstrate a private high-speed CRBG scheme based on an MZM electro-optic self-feedback loop for synchronized wideband physical entropy sources, which effectively enhances the rate of physical entropy sources and the hardware

key space. The results show that the entropy source rate of the synchronized wideband physical entropy source is greatly extended to ~ 25 GHz. Meanwhile, the synchronization between Alice and Bob still maintains a high quality of 0.986, and the residual correlation between the driving signal and the response output synchronization broadband physical entropy source is effectively suppressed. Based on this scheme, a high-speed CRBG of up to 5.3 Gb/s has been achieved successfully. Combined with the commercial module, the improved hardware key space in the practical application is considered. By adding a hardware module for post-processing, the $\sim 2^{42}$ hardware key space is enhanced, which greatly improves the privacy of the physical entropy source. This scheme provides a promising strategy for high-speed private CRBG between physical entropy sources based on electro-optical signal processing in the future and has broad application prospects in future high-speed secure communication systems.

Author Contributions: Conceptualization, C.H. and Z.G.; methodology, S.W. and Z.G.; software, C.H. and X.G.; validation, C.H.; formal analysis, C.H. and W.G.; investigation, X.G. and W.G.; resources, X.G. and S.W.; data curation, C.H. and S.W.; writing—original draft preparation, C.H. and B.S.; writing—review and editing, C.H. and X.G.; supervision, Z.G., Y.W. and Y.Q.; project administration, Z.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China under Grant 2018YFB1801301, in part by the National Natural Science Foundation of China under Grants U2001601, U22A2087, 11904057, and 62004047, in part by the Basic and Applied Basic Research Project of the Guangzhou Basic Research Program under Grant 202102020506, in part by the Research and Development Plan in Key Areas of Guangdong Province under Grant 2018B010114002, and in part by the Guangdong Introducing Innovative and Entrepreneurial Teams of The Pearl River Talent Recruitment Program under Grant 2019ZT08X340. (Corresponding author: Zhensen Gao).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: 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.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Eastlake, D., 3rd; Schiller, J.; Crocker, S. Randomness Requirements for Security . Technical Report. No. rfc4086. 2005.
2. Bucci, M.; Germani, L.; Luzzi, R.; Trifiletti, A.; Varanunovo, M. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC. *IEEE Trans. Comput.* **2003**, *52*, 403–409. [\[CrossRef\]](#)
3. Petrie, C.S.; Connelly, J.A. A Noise-Based IC Random Number Generator for Applications in Cryptography. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2000**, *47*, 615. [\[CrossRef\]](#)
4. Stojanovski, T.; Pihl, J.; Kocarev, L. Chaos-based random number generators. Part II: Practical realization. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2001**, *48*, 382–385. [\[CrossRef\]](#)
5. Wayne, M.A.; Kwiat, P.G. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express* **2010**, *18*, 9351–9357. [\[CrossRef\]](#) [\[PubMed\]](#)
6. Li, X.Z.; Chan, S.C. Random bit generation using an optically injected semiconductor laser in chaos with oversampling. *Opt. Lett.* **2012**, *37*, 2163. [\[CrossRef\]](#) [\[PubMed\]](#)
7. Zhang, Y.; Zhang, J.; Zhang, M.; Wang, Y. 2.87-Gb/s random bit generation based on bandwidth-enhanced chaotic laser. *Chin. Opt. Lett.* **2011**, *9*, 031404. [\[CrossRef\]](#)
8. Nguimdo, R.M.; Verschaffelt, G.; Danckaert, J.; Leijtens, X.; Bolk, J.; Guy, V. Fast random bits generation based on a single chaotic semiconductor ring laser. *Opt. Express* **2012**, *20*, 28603–28613. [\[CrossRef\]](#)
9. Koizumi, H.; Morikatsu, S.; Aida, H.; Nozawa, T.; Kakesu, I.; Uchida, A.; Yoshimura, K.; Muramatsu, J.; Davis, P. Information-theoretic secure key distribution based on common random-signal induced synchronization in unidirectionally-coupled cascades of semiconductor lasers. *Opt. Express* **2013**, *21*, 17869–17893. [\[CrossRef\]](#)
10. Kanter, I.; Butkovski, M.; Peleg, Y.; Zigzag, M.; Kinzel, W. Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography. *Opt. Express* **2010**, *18*, 18292–18302. [\[CrossRef\]](#)
11. Shao, W.; Fu, Y.; Cheng, M.; Deng, L.; Liu, D. Chaos Synchronization Based on Hybrid Entropy Sources and Applications to Secure Communication. *IEEE Photonics Technol. Lett.* **2021**, *33*, 1038–1041. [\[CrossRef\]](#)

12. Yoshimura, K.; Muramatsu, J.; Davis, P.; Harayama, T.; Okumura, H.; Morikatsu, S.; Aida, H.; Uchida, A. Secure Key Distribution Using Correlated Randomness in Lasers Driven by Common Random Light. *Phys. Rev. Lett.* **2012**, *108*, 070602. [[CrossRef](#)] [[PubMed](#)]
13. Li, X.Z.; Li, S.S.; Chan, S.C. Correlated Random Bit Generation Using Chaotic Semiconductor Lasers under Unidirectional Optical Injection. *IEEE Photonics J.* **2017**, *9*, 1–11. [[CrossRef](#)]
14. Fu, Y.; Cheng, M.; Jiang, X.; Deng, L.; Ke, C.; Fu, S.; Tang, M.; Zhang, M.; Shum, P.; Liu, D. Wavelength division multiplexing secure communication scheme based on an optically coupled phase chaos system and PM-to-IM conversion mechanism. *Nonlinear Dyn.* **2018**, *94*, 1949–1959. [[CrossRef](#)]
15. Argyris, A. Sub-Tb/s Physical Random Bit Generators Based on Direct Detection of Amplified Spontaneous Emission Signals. *J. Light. Technol.* **2012**, *30*, 1329–1334. [[CrossRef](#)]
16. Shen, Y.; Tian, L.; Zou, H. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A* **2010**, *81*, 89–95. [[CrossRef](#)]
17. Symul, T.; Assad, S.M.; Lam, P.K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* **2011**, *98*, 145. [[CrossRef](#)]
18. Guo, H.; Tang, W.; Yu, L.; Wei, W. Truly Random Number Generation Based on Measurement of Phase Noise of Laser. *Phys. Rev. E Stat. Nonlinear Soft Matter Phys.* **2010**, *81*, 051137. [[CrossRef](#)]
19. Kanter, I.; Aviad, Y.; Reidler, I.; Cohen, E.; Rosenbluh, M. An optical ultrafast random bit generator. *Nat. Photonics* **2010**, *4*, 58–61. [[CrossRef](#)]
20. Mbe, J.; Atchoffo, W.N.; Tchitnga, R.; Wofo, P. Dynamics of Time-delayed Optoelectronic Oscillators with Nonlinear Amplifiers And Its Potential Application to Random numbers Generation. *IEEE J. Quantum Electron.* **2021**, *57*, 1–7.
21. Zhao, A.; Jiang, N.; Wang, Y.; Liu, S.; Qiu, K. Correlated random bit generation based on common-signal-induced synchronization of wideband complex physical entropy sources. *Opt. Lett.* **2019**, *44*, 5957. [[CrossRef](#)]
22. Gao, Z.; Wu, S.; Deng, Z.; Huang, C.; Gao, X.; Fu, S.; Li, Z.; Wang, Y.; Qin, Y. Private correlated random bit generation based on synchronized wideband physical entropy sources with hybrid electro-optic nonlinear transformation. *Opt. Lett.* **2022**, *47*, 3788–3791. [[CrossRef](#)] [[PubMed](#)]
23. Sciamanna, M.; Shore, K.A. Physics and Applications of Laser Diode Chaos. *Nat. Photonics* **2015**, *9*, 151–162. [[CrossRef](#)]
24. Wang, L.; Wang, D.; Gao, H.; Guo, Y.; Wang, Y.; Hong, Y.; Shore, K.A.; Wang, A. Real-Time 2.5-Gb/s Correlated Random Bit Generation Using Synchronized Chaos Induced by a Common Laser with Dispersive Feedback. *IEEE J. Quantum Electron.* **2020**, *56*, 1–8. [[CrossRef](#)]
25. Bhm, F.; Sahakian, S.; Dooms, A.; Verschaffelt, G.; Sande, G. Stable High-Speed Encryption Key Distribution via Synchronization of Chaotic Optoelectronic Oscillators. *Phys. Rev. Appl.* **2020**, *13*, 064014. [[CrossRef](#)]
26. Hirano, K.; Yamazaki, T.; Morikatsu, S.; Okumura, H.; Davis, P. Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers. *Opt. Express* **2010**, *18*, 5512–5524. [[CrossRef](#)]
27. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; NIST Special Publication: Gaithersburg, MD, USA, 2001.
28. Yamamoto, T.; Oowada, I.; Yip, H.; Uchida, A.; Yoshimori, S.; Yoshimura, K.; Muramatsu, J.; Goto, S.I.; Davis, P. Common-chaotic-signal induced synchronization in semiconductor lasers. *Opt. Express* **2007**, *15*, 3974–3980. [[CrossRef](#)]
29. Wang, A.; Yang, Y.; Wang, B.; Zhang, B.; Wang, Y. Generation of wideband chaos with suppressed time-delay signature by delayed self-interference. *Opt. Express* **2013**, *21*, 8701–8710. [[CrossRef](#)]
30. Hong, Y.; Spencer, P.S.; Shore, K.A. Wideband Chaos with Time-Delay Concealment in Vertical-Cavity Surface-Emitting Lasers with Optical Feedback and Injection. *IEEE J. Quantum Electron.* **2014**, *50*, 236–242. [[CrossRef](#)]
31. Wang, D.M.; Wang, L.S.; Guo, Y.Y.; Wang, Y.C.; Wang, A.B. Key space enhancement of optical chaos secure communication: Chirped FBG feedback semiconductor laser. *Opt. Express* **2019**, *27*, 3065. [[CrossRef](#)]
32. Sakuraba, R.; Iwakawa, K.; Kanno, K.; Uchida, A. Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers. *Opt. Express* **2015**, *23*, 1470. [[CrossRef](#)]
33. Wang, A.; Wang, L.; Pu, L.; Wang, Y. Minimal-post-processing 320-Gbps true random bit generation using physical white chaos. *Opt. Express* **2017**, *25*, 3153–3164. [[CrossRef](#)] [[PubMed](#)]
34. Sasaki, T.; Kakesu, I.; Mitsui, Y.; Rontani, D.; Inubushi, M. Common-signal-induced synchronization in photonic integrated circuits and its application to secure key distribution. *Opt. Express* **2017**, *25*, 26029–26044. [[CrossRef](#)] [[PubMed](#)]
35. Pu, L.; Zhang, J.; Sang, L.; Liu, X.; Wang, Y. Real-time online photonic random number generation. *Opt. Lett.* **2017**, *42*, 2699–2702.