40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission

Guo, Ya; Cai, Qiang; Li, Pu; Jia, Zhiwei; Xu, Bingjie; Zhang, Qianwu; Zhang, Yamei; Zhang, Ruonan; Gao, Zhensen; Shore, K. Alan; Wang, Yuncai

APL Photonics

DOI:
10.1063/5.0040250

Published: 01/06/2021

Peer reviewed version

40 Gb/s Quantum Random Number Generation Based on Optically Sampled Amplified Spontaneous Emission

Ya Guo,[1,2,†] Qiang Cai,[2,†] Pu Li,[2,3,4,*] Zhiwei Jia,[2] Bingjie Xu,[5] Qianwu Zhang,[4] Yamei Zhang,[6] Ruonan Zhang,[1] Zhensen Gao,[3] K. Alan Shore,[7] and Yuncai Wang[3]

[1]*School of Electronics and Information, Northwestern Polytechnical University, Xi'an, 710072, China*
[2]*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan, 030024, China*
[3]*School of Information Engineering, Guangdong University of Technology, Guangzhou, 510006, China*
[4]*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai, 200444, China*
[5]*Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China*
[6]*Key Laboratory of Radar Imaging and Microwave Photonics, Ministry of Education, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*
[7]*School of Electronic Engineering, Bangor University, Wales LL57 1UT, U.K.*
[†]*These authors contributed equally to this work*
**Author to whom correspondence should be addressed: lipu8603@126.com*

Abstract: We present a photonic approach for fast quantum random number generation based on optically sampled amplified spontaneous emission (ASE). This approach utilizes a terahertz optical asymmetric demultiplexer (TOAD) to sample the ASE and then digitize the sampled optical pulses into random bits using a multi-bit parallel comparator (COM). A proof-of-concept experiment demonstrates that, 40 Gb/s random bits with verified randomness can be obtained using our method. The current generation rate is mainly limited by the bandwidth of the available ASE source.

I. INTRODUCTION

True random numbers play crucial roles in various areas, especially for high-tech communication security. Quantum random number generators (QRNGs), extracting the intrinsic randomness from the nondeterministic nature of quantum physics, can provide truly unpredictable and irreproducible random numbers.[1,2] Owing to such unique advantage, various quantum entropy sources (QESs) have been proposed and utilized to develop QRNGs, including measuring laser phase fluctuations,[3-5] photon events,[6-11] quantum vacuum fluctuations,[12,13] and the amplified spontaneous emission (ASE).[14-20]

Among them, the ASE-based QRNGs have attracted tremendous attention due to their advantages in achieving high generation rates. For instance, Williams *et al.* pioneered the work of fast random number generations based on the filtered ASE from a fiber amplifier and produced a 12.5 Gb/s random bits sequence using threshold comparison and off-line XOR decorrelation techniques in 2010.[14] In 2014, our group exploited a similar threshold comparison technique by merging of an electrical single-bit analog-to-digital converter (ADC) and a XOR gate and successfully achieved a 2.5 Gb/s real-time QRNG utilizing the filtered ASE from a super-luminescent diode (SLD).[15] In 2017, Xu *et al.* realized a 1.2 Gb/s real-time generation rate using an electrical multi-bit ADC to digitalize the ASE from a super-luminescent light emitting diode (SLED).[16] More recently, a continuous-variable random-number generator using the ASE from an Er-doped fiber successfully achieved a maximum generation rate of 2.5 Gb/s.[17]

For faster bits rate, some excellent schemes using electrical ADCs and extensive post-processes have been demonstrated.[18-20] The latest research indicates that the generation rate could be enhanced to several tens of Gb/s, even on the order of sub-Tb/s. For instance, Li *et al.* implemented two parallel channels of random bits generation (10 Gb/s in per channel) utilizing spectrally-sliced ASE from a single SLD.[18] Guo *et al.* realized a 280 Gb/s QRNG using a digital logic method to extract 8 bits from per sample at the sampling rate of 40 GSa/s.[19] Argyris *et al*. reported a 560 Gb/s QRNG by means of multi-bit representation form to digitize the sampled ASE.[20]

However, it should be noticed that these ultrafast QRNGs based on electrical single-bit or multi-bit ADCs and advanced data post-processing methods are merely implemented in theory through off-line extraction from experimental temporal waveforms of the ASE, and thus are not truly real-time outputs. Up to now, to the best of our knowledge, 2.5 Gb/s remains the fastest real-time rate realized by all the ASE-based QRNGs with verified randomness. This is far from what is desirable for practical applications, because current communication rates have reach 40 Gb/s or even higher.

One of the ultimate hindrances in the actual implementation of the QRNGs with faster real-time bit rate is the timing jitter of electrical ADCs driven by electronic sampling clocks from radio frequency (RF) oscillators. This is because the current RF oscillators inevitably have a large timing jitter and will introduce serious sampling errors between ideal sampling points and real sampling points.[21,22] Up to now, the state-of-the-art electronic clocks deliver at the level of 100 fs of RMS jitter even in the 100 MHz low frequency range, which will rapidly deteriorate with the enhancement of operation frequencies and is increasingly difficult to reduce the jitter. Moreover, the severer the electronic jitter is, the larger the sampling deviation will be and thus the more serious the signal distortion is.[22,23] Especially, when the sampling rate is high in the range of 10 GHz, even small timing jitter can destroy the output code waveform and its associated eye diagram from the electrical ADC. Seriously, this may cause that the quantized waveform cannot be coded correctly into binary random bit sequences. In addition, it is rather difficult to further reduce this electronic jitter. Expectations for further electrical ADCs suggest that, it will take at least a decade to improve the electronic jitter performance by an order of magnitude.[24] In consequence, the practical

physical bandwidth of high-speed electrical ADCs is commonly limited to few GHz.

Using optical sampling can overcome this limitation caused by the electronic timing error.[23-25] This is because when optical pulses with ultralow jitter at the level of femtosecond (fs) generated by a mode-locked laser (MLL) are used as the sampling clock, 3 ~ 4 orders of magnitude lower in jitter can be reduced than that of the traditional electrical clock. Just the reduction of the timing jitter brings that the effective quantization resolution (*i.e.*, effective number of bits, ENOB) and the available input analog signal bandwidth can be greatly enhanced.[24] Quantitatively, it can also be seen from Ref. 24 that when the jitter is reduced to the level of 10 fs, the effective quantization resolution and the analog bandwidth at least has the potential to be enhanced to the level of 8 bits and 10 GHz, respectively.

This inspires us to propose and experimentally demonstrate a photonics-based scheme for fast multi-bit quantum random number generation. Specifically, the sampling of the output ASE from a SLD is firstly done in the optical domain through a terahertz optical asymmetric demultiplexer (TOAD)-based optical sampler. Then, the optically sampled pulses are converted continuously into random bit streams in binary format by an 8-bit parallel comparator built-in a high-speed real-time serial data analyzer. Finally, 4 least significant bits (LSBs) retention is implemented at 10 GSa/s sampling rate, and thus 40 Gb/s (=10 GSa/s×4 bits) random bit sequences can be successfully extracted.

To the best of our knowledge, this proposal is the first combination of the ASE signals and a photonic sampled ADC. In comparison with the previous QRNG schemes, there exist at least two significant advantages to our approach. (i) Using an optical sampler driven by ultrashort mode-locked optical pulses can overcome the electronic jitter issue confronted by electrical ADCs. This is because the current timing jitter of the MLL is now about 10 fs or even lower.[24] Under this condition, the ASE noise can be optically sampled with higher rate and accuracy.[26,27] (ii). Compared with an 8-bit ADC, the 8-bit parallel comparator in our method does not contain the S/H circuit in its front end. Thus, the 8-bit parallel comparator does not make the function of sampling, but only quantize the sampled random pulses from the TOAD with an ultralow timing jitter into binary bit sequences. In this way, the timing jitter issue confronted by the electrical ADC can be solved efficiently.

Moreover, the QRNG rate with our scheme is jointly determined by the number of retained LSBs and the optical sampling rate. In this proof-of-principle experiment, the optical sampling rate is only set at 10 GSa/s controlled by the pulse-repetition rate of the MLL used. Considering the ultrafast response rate of the TOAD-based optical sampler, our QRNG is expected to achieve a real-time bit rate up to tens or even hundreds of Gb/s when the bandwidth of the available ASE signals is sufficiently broad. We believe that this work will motivate more implementation of ultrafast QRNGs with associated all-optical signal processing technologies in near future.

II. EXPERIMENTAL SETUP AND RESULTS

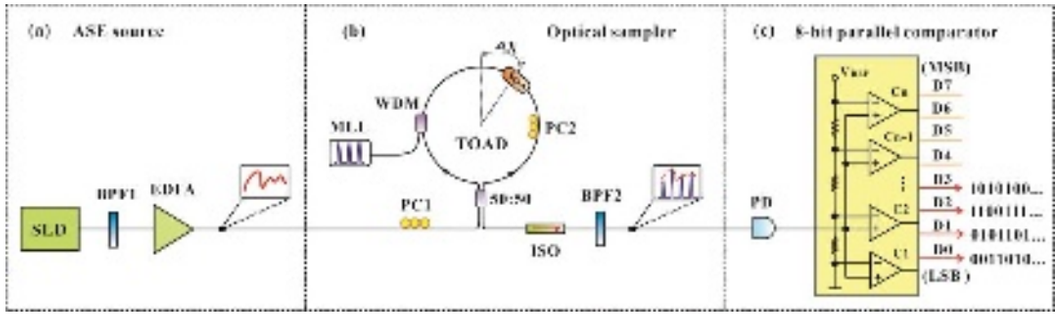


FIG. 1. Schematic diagram of the proposed fast QRNG based on optically sampled ASE: (a) ASE source, (b) Optical sampler, and (c) 8-bit parallel comparator. SLD, super-luminescent diode; EDFA, Er-doped fiber amplifier; BPF1, BPF2, optical band-pass filters; MLL, mode-locked laser; WDM, wavelength division multiplexer coupler; SOA, semiconductor optical amplifier; PC1, PC2 polarization controllers; 50:50, 50:50 optical coupler; TOAD, terahertz optical asymmetric demultiplexer; ISO, optical isolator; PD, photodetector; LSB, least significant bit; MSB, most significant bit.

Figure. 1 is the experimental schematic for implementing the proposed fast QRNG based on optically sampled the ASE noise emitted from a SLD. The whole setup mainly consists of three crucial components: (a) ASE source, (b) Optical sampler, and (c) 8-bit parallel comparator, as depicted in Fig. 1. The 8-bit parallel comparator used in experiments is provided by a 36 GHz real-time serial data analyzer (Lecroy, LabMaster10-36Zi, 80 GSa/s sampling rate, 8-bit vertical resolution). Note that the external trigger clock applied in our system is a high-level DC signal so that the sampling function will not be executed during our quantization process. In this way, the real-time serial data analyzer can be used as an 8-bit comparator. In addition, we want to point that utilizing discrete ADC devices (such as AAD08S010G from AcelaMicro and AD9213 from ADI) can also realize the function of a multi-bit comparator as long as the trigger clock is replaced by a high-level DC signal source.

A. ASE source

In our experiments, we selected the ASE noise from the SLD (Thorlabs, SLD1005S) with a 3-dB optical spectrum width of more than 50 nm centered at 1550 nm as the random entropy source. The laser was operated by applying a constant 360.0 mA current (~ 4.0 times the laser threshold) while its working temperature was maintained at 24°C with variations less than 0.1°C. In such case, the output power of the SLD is about 13 mW. Firstly, the ASE noise is filtered by an optical band-pass filter (BPF) working at a center wavelength of 1553.7 nm with a 3-dB bandwidth of 0.6 nm. Then, an EDFA (Keopsys, CEFA-C-HB-CPB30) after the BPF is used to adjust the power of the ASE signal and make it efficiently injected into the optical sampling device (TOAD).

From Fig. 2(a), we can observe that the optical spectrum of the SLD is wide enough to be spectrally demultiplexed into many statistically independent quantum noise sources. Fig. 2(b) illustrates that the RF spectrum of the filtered ASE is very flat over a wide bandwidth range,

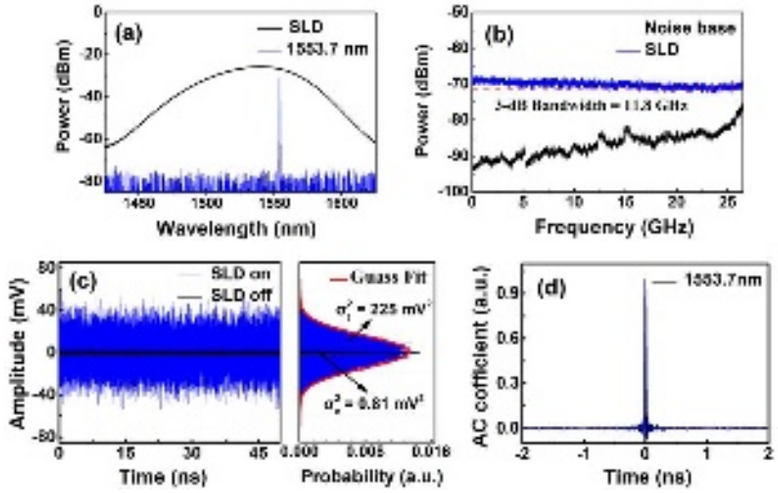


FIG. 2. Schematic Characteristics of the filtered ASE. (a) The optical spectra of the SLD (the black line) and the spectrally-sliced channel (the blue line). (b) The RF spectrum of the filtered ASE (the blue line) and the electrical background noise (the black line). (c) The temporal waveform and the amplitude distribution of the filtered ASE and the classical noise (the red line is the Gaussian fitted curve). (d) The autocorrelation trace of the filtered ASE temporal waveforms.

which is about 11.8 GHz calculated utilizing the 3-dB bandwidth definition. This kind of high bandwidth level is highly beneficial for subsequent ultrafast random bits extraction. Further, the characteristic of the amplitude distribution of the filtered ASE and the classical noise temporal waveforms are explored. As depicted in Fig. 2(c), the plots labeled "SLD on" show total noises (*i.e.,* the quantum noise and the classical noise), and the plots labeled "SLD off" show the case where only classical noises are contained (*i.e.,* noise sources are mainly contributed from background detections and electronic noises such as the EDFA, the SOA, the photodetector, and the parallel comparator, etc.). Their corresponding probability distributions are also shown in the right side in Fig. 2(c), in which the red line is the Gaussian fitted curve of the obtained total noise amplitude. From the statistical results, one can observe clearly that its amplitude exhibits a Gaussian-like distribution. Such characteristic is strongly suggestive of enabling the production of un-biased and high-quality random bits. Finally, the signal autocorrelation trace of the filtered ASE temporal waveforms is plotted in Fig. 2(d) with a sample size of 1.6 Mbits. Obviously, there is no dominant correlation peak. This positive feature is mainly due to the fact that the ASE signals are essentially a fundamental quantum phenomenon. In our experiments, the optical spectra are measured by an optical spectrum analyzer with a resolution of 0.02nm (YOKOGAWA, AQ6370C). The temporal waveform and the electric power spectrum are detected by a 36 GHz real-time digital oscilloscope (LabMaster10-36Zi, 80 GS/s sampling rate) and a 26.5 GHz radio-frequency spectrum analyzer (Agilent N9020A, 3 MHz RBW, 3 KHz VBW) via a 45 GHz PD (U^2T, XPDV2120RA).

In practice, even though the measured quantum signal (the source of genuine randomness) in the coherent detection-based QRNGs is inevitably mixed with classical noise,[28,29] The genuine randomness still can be extracted from the mixture of quantum signal and classical noise. The premise in terms of satisfying the extraction requirement of signal randomness is

not very difficult. When the signal intensity is sufficiently larger than the classical noise, then the contribution of the latter can be neglected.[30-34] Based on this fact, the method of using a key parameter, quantum-classical noise ratio (QCNR) has been widely adopted to quantify the amount of quantum noise to the amount of classical noise. In this regard, we can describe the variance of the whole system output voltage from the detector as $\sigma_t^2 = \sigma_q^2 + \sigma_c^2$, as shown in Fig. 2(c) where σ_q^2 and σ_c^2 are measured variances of the ASE noise and the classical noise, respectively. The calculated results show that the total measured intensity noise σ_t^2 is 225 mV^2, and σ_c^2 is 0.81 mV^2, which is mainly derived from the electronic noise of the detector and quantizer. Further, the quantum variance is obtained as σ_q^2 = 224.19 mV^2. Then the QCNR [QCNR = $10\log_{10}(\sigma_q^2/\sigma_c^2)$] is achieved at a fixed laser power, the corresponding QCNR is about 23.8 dB. In other words, the measured quantum signal produced by the SLD is more than higher 23.8 dB than the classical noise. In this case, the corresponding maximum ratio γ ($\gamma = 1 - \sigma_c^2/\sigma_t^2$) of the ASE noise to the total noise is 99.64 %.[31-34] These statistical results indicate that the ASE noise is dominate in our system, which guarantees the security and quality of the exacted quantum random bits.

B. Optical sampler

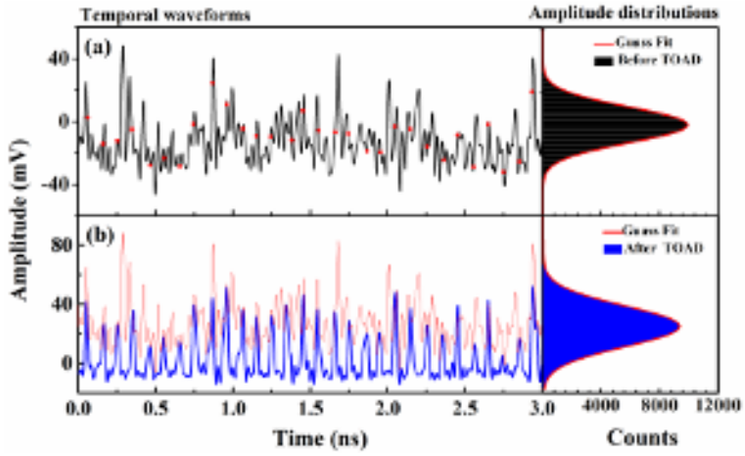


FIG. 3. Optical sampling characteristics. (a) Continuous-time ASE noise temporal waveforms to be sampled and (b) discrete-time ASE pulses temporal waveforms after the optical sampling procedure.

In the sampling part [Fig. 1(b)], a simple TOAD-based optical sampler is introduced in our proof-of-principle experiment. The TOAD is an all-optical switch based on the Sagnac interferometer principle. It is composed of a fiber loop mirror with additional intra-loop elements: a 3-dB optical coupler, a wavelength division multiplexer (WDM), a polarization controller (PC), an optical band-pass filter (BPF), and a nonlinear semiconductor optical amplifier (SOA) as the nonlinear element, that is offset from the loop midpoint by a distance Δx. The operation principle of the TOAD can be described with the help of Fig. 1(b). A train of ultrashort optical clock pulses from the MLL are coupled into TOAD by a WDM as the control light; at the same time, the sampled continuous-wave as the signal light enters the loop via a 50:50 optical coupler and splits into two signals: a clockwise (CW) and a counterclockwise (CCW) propagating signal. Because the SOA is located at a certain distance Δx away from the fiber ring center,[35-37] the two counter-propagation light will successively arrive at the SOA, and thus forming a delay window (a sampling or switching window).

Specifically, when a control optical clock pulse reaches SOA, SOA reaches gain saturation state, and then gradually recovers. As a result, the two counter-propagation signal components experience a different phase modulation when they pass through the device before and after the clock pulse, respectively. Otherwise, they are affected by the same phase modulation. The two different conditions allow us to obtain two different transmission values, and thus, forming a sampling window with a time length $\Delta t = 2\Delta x/vg$ (vg represents the group-velocity of the two counterpropagating signal in the fiber loop). During operation, the sampling window is opened periodically with the arrival of optical clock pulse, so the input waveform can be sampled at the clock repetition. Finally, using a BPF, we can separate the sampled output from the optical clock because their operating wavelengths are different. In our study, the filtered amplified ASE is first coupled into the TOAD by a 50:50 optical coupler and then split into two equal beams in the CW and CCW direction, respectively. Meanwhile, a series of picosecond optical clock pulses originating from an ultrafast MLL are injected into the TOAD via a wavelength division multiplexer (WDM), which can periodically switch the sampling gate so that the ASE noise will be sampled at the clocking rate. After that, the separation of the sampled ASE pulses is finally realized by using a BPF near the output port of the TOAD.

In this experiment, the nonlinear SOA (Kamelian, SOA-NL-L1-C-FA) with a gain recovery time of 25 ps is biased at 300 mA and operates at a peak gain wavelength of 1550 nm, a 3-dB bandwidth of 64 nm. The MLL (Pritel, UOC-05-14G-E) with a timing jitter smaller than 50 fs operates at 10 GHz and its wavelength is tuned to be 1551.2 nm. The BPF works at a center wavelength of 1553.7 nm with a 3-dB bandwidth of 0.6 nm, corresponding to that of the sampled output, so the sampled output can be separated from the sampling optical clock [as shown in the bottom right of Fig. 1(b)]. Quantitatively, the sampling output P_{out} roughly satisfies $P_{out} \propto P_{in}[G_{CW} + G_{CCW} - 2\cdot(G_{CW}\cdot G_{CCW})^{1/2}\cdot\cos(\Delta\varphi)]$, where P_{in} represents the power of the ASE noise signal to be sampled, and G_{CW} and G_{CCW} denote the gains which CW and CCW ASE noise signals achieved through the SOA, respectively. The phase shift $\Delta\varphi$ experienced by CW and CCW is controlled by the optical clock. The constructive interference occurs only when $\Delta\varphi$ equals π and, thus, the ASE noise signal can be sampled. To guarantee this π phase shift, the average power of optical clock pulse is set about -10 dBm in our experiment. By comparing Fig. 3(a) and Fig. 3(b), one can observe clearly that the continuous-time envelope of the sampled analog ASE noise [Fig. 3(a)] match well with the peaks of the discrete-time ASE pulses [Fig. 3(b)], which confirms the high-fidelity of the sampling operation. Herein, to illustrate the sampling results clearly, the sampled ASE noise are divided into two beams by a 90:10 optical coupler: 90 % is fed into the TOAD to be sampled and subsequent quantization, whilst 10 % is used as a reference path, which is convenient for us to compare with the final sampling results [*i.e.*, red temporal waveforms in Figs. 3(b)]. Both beam signals are synchronously recorded by a multi-channel real-time oscilloscope. However, one point should be noticed here is that in order to better real-time synchronously observe the two beam optical signals, it is necessary to select appropriate optical delay lines to adjust the transmission length of the two beam optical signals.

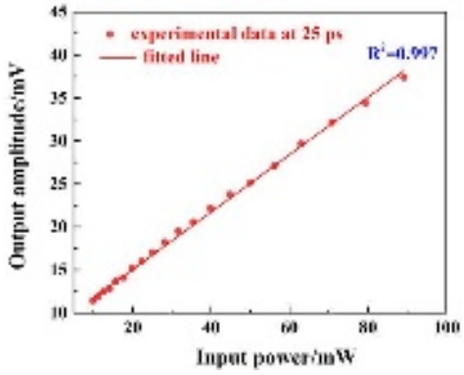


FIG. 4. Linearity evaluation of the TOAD-based all-optical sampler.

In addition, the sampling linearity has also been evaluated in our experiment to quantitatively estimate the sampling fidelity. Fig. 4 depicts the relationship between the amplitude of the sampled output signal and the power of the input signal to be sampled in our TOAD-based all-optical sampler. The solid mark is experimental data with a fitted line. After calculation, the linearity R^2 of the sampling process is as high as 0.997. This means a high fidelity.

In fact, the applied optical sampler (TOAD) can not only achieve a high-fidelity sampling, but also improve the amplitude of the sampled ASE noise due to the gain compensation effect of the SOA. The sampled ASE noise with amplified amplitude (that is, when the output is an optically sampled pulse, the corresponding pulse amplitude will fluctuate largely) is highly beneficial for subsequent quantization and random number exaction. To prove the correctness of this point, we have made several relevant statistical analysis on the amplitude distributions of the ASE signal before and after the TOAD as shown in Fig. 3. To clarify this point more directly, we plot the amplitude distribution of the ASE noise before and after the optical sampler as shown in Fig. 5. The amplitude distribution is plotted using 1.6 million data points. From it, one can observe that there exists a good linearity between the original and the optically sampled noise. After calculation, their evolution relationship can be expressed into Y=2.48X+51.56, where X and Y represent the time series of the noise before and after the optical sampling, respectively. In addition, we evaluate the deviations between the ideal and the real sampled points using the mean square error (MSE). Calculated results indicate that the MSE is at a very low level about 4.3×10^{-4}. Thus, we confirm that our optical sampling method can significantly improve the amplitude of the sampled ASE signal, which is very helpful to avoid the participation of complex post-processing.

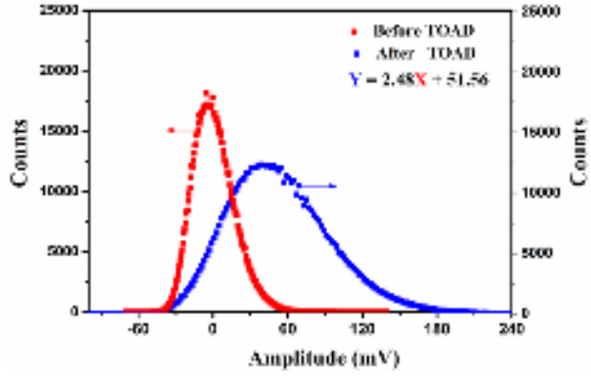


FIG. 5 Statistical distribution of the ASE noise amplitudes before and after optical sampling with the

TOAD.

C. 8-bit parallel comparator

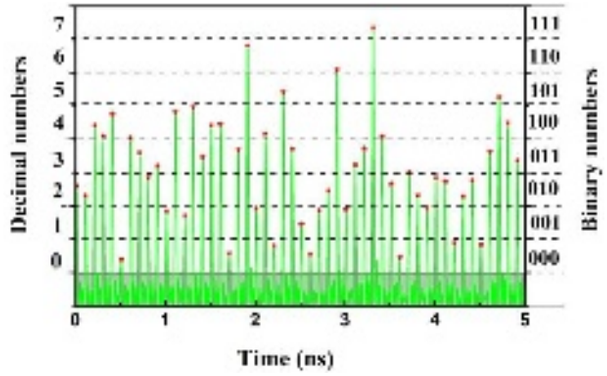


FIG. 6. Quantization principle of the optically sampled ASE pulses train (take a 3-bit quantization as an example).

An 8-bit parallel comparator embedded in the 36 GHz real-time serial data analyzer has been employed to quantize the optically sampled pulses. Here, to clearly explain the quantizing process, we take a 3-bit quantization as an example to illustrate the operation principle in our experiment. As shown in Fig. 6: the green curves represent the resulting time-series of the sampled pulses; the seven gray dotted lines indicate the seven different decision thresholds of a 3-bit quantizer. The number of recorded samples is 1.6 Mbits. Combined with these decision thresholds, the peak point of the sampled pulses (marked with red * in Fig. 6) can be divided into 3-bit binary codes, which agrees strongly with the corresponding threshold interval, as labeled in the vertical coordinate on the right side of the Fig. 6. As expected, the entire amplitude range of the sampled pulses, under such condition, will be mapped into 8 strips. Then, in accordance with binary coding, each strip from bottom to top can be coded into "000", "001", "010", "011", "100", "101", "110" and "111", respectively. The 3-bit binary codes shown in Fig. 6 from right column to left column correspond to D_0, D_1 and D_2 output from the 8-bit parallel comparator in Fig. 1(c). Thus, for a 3-bit quantizer, D_0 and D_2 are considered as the LSB and the most significant bit (MSB), respectively. The decimal digitization levels corresponding to the 3-bit binary codes are labeled in the vertical coordinate on the left side of the Fig. 6.

III. QUANTUM RANDOMNESS EVALUATION AND EXTRACTION

As mentioned earlier, the raw random bits from our QRNG are contributed by both the quantum noise and the classical noise. Up to date, extensive methods for extracting the randomness have been applied to quantum random bit generation such as the min-entropy evaluation[28,29], the Toeplitz-hashing algorithm[30,31], the Trevisan's extractor[32,38,39], and even the constructed physical model[40,41]. Herein, the extractable randomness of the raw data X is quantified by the worst-case min-entropy conditioned on classical side information E [31,33]:

$$H_{\min}(X|E) = -\log_2[\max_{e\in R}\max_{x_i\in X} P_{X|E}(x_i \mid e)] \quad (1)$$

Where $P_{X/E}(x_i|e)$ is the discretized conditionally probability distribution of $x_i \in$ X. When the measurement output follows Gaussian distribution, Eq. (1) can be simplified as

$$H_{\min}(X \mid E) = -\log_2[\max(c_1, c_2)] \quad (2)$$

with $c_1 = erf(\frac{\delta}{2\sqrt{2}\sigma_Q})$ and $c_2 = \frac{1}{2}[erf(\frac{e_{\max} - R + 3\delta/2}{\sqrt{2}\sigma_Q}) + 1]$. R (*i.e.*, $R = 4.4\sigma_Q$) equals to half of the input of the quantizer module and $\delta = 2R/(2^n)$, where n (*i.e.*, n = 8) is the sampling precision. σ_Q indicates the value of the standard deviation of quantum noise. The maximum classical noise excursion is chosen to be $e_{\max} = 5\sigma_E$ (σ_E^2 = the variances of classical noise) with 99.9999% confidence level.[31,33] We simplify the analysis progress and ensure that the system works under safety condition that $c_1 = 0.0137 \geq c_2$, in which the comparison between c_1 and c_2 will indicate whether the min-entropy evaluation utilizes the correct maximum guessing probability. In this case, the $H_{\min}(X|E)$ is estimated to be 6.19 bits per sample.

In the post-processing stage, the Toeplitz algorithm is employed as the randomness extractor to eliminate the classical noise and improve the statistical quality of the random numbers.[42-45] Given $m \times n$ binary Toeplitz matrix, m random bits are extracted by multiplying the Toeplitz matrix with n raw bits. A true random sequence with length of $n + m$ -1 bits is required and prestored to build the $m \times n$ binary Toeplitz matrix. In order to further optimize the extracting process, we choose m = 1024 and n = 1360 > 1024 × 8/6.19. According to the leftover hash lemma $m = n \cdot H_{\min}(X \mid E)/8 - 2\log_2(1/\varepsilon)$, the corresponing security parameter ε is calculated as 2^{-14}. Finally, the bit rate of the presented QRNG has the potential to be over 40 Gbps.

Note, a true random bit stream should be strictly un-biased and mutually independent. Figs. 7(a) and 7(b) depict the calculated results of the statistical bias and the normalized autocorrelation (AC) coefficients of the achieved 40 Gb/s binary random bit stream, respectively. Both the bias and the AC function are estimated utilizing the normalized Gaussian distribution estimation N (0, σ^2). Further, one can see clearly that both the bias and the serial AC coefficients are both below their three-standard-deviation indicated as $3\sigma_e = (3N^{-1/2})/2$ and $3\sigma_c = (3N^{-1/2})$ [the red solid lines in Figs. 7(a) and 7(b)], which means that the achieved random bit sequences have good statistical randomness.

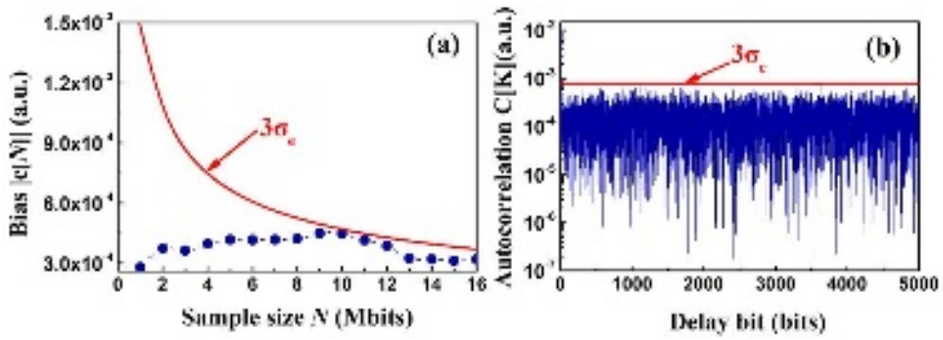


FIG. 7. (a) Bias |e[N]| versus the sample size of the generated 40 Gb/s random bit stream; The red line in (a) is its three-standard-deviation line, $3\sigma_e = (3N^{-1/2})/2$ where n = 1, 2, 3, …, 16Mbits. (b) Autocorrelation coefficient C[K] as a function of the delay bit K for a 16 × 10^6 bit.

Lastly, to better qualify the statistical randomness of the generated bit sequences, we use the state-of-the-art National Institute of Standards and Technology (NIST Special Publication 800-22) test suite with 15 statistical test items[46] to examine the obtained random bits (a 40 Gb/s sequence by reserving 4-LSBs sampled at 10 GSa/s). As advised by the NIST, each test is performed using 1000 × 1 Mbits with a statistical significance level $\alpha = 0.01$. The test criterion for "Success" is that the *P*-value (uniformity of p-values) should be larger than 0.0001 and the proportion should be within the range of 0.99 ± 0.0094392. Note, the *P*-value is the probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by NIST tests. For tests that return multiple *P*-values and proportions, the worst case is depicted in Fig. 8, in which the left and right ordinates represent the *P*-value and the proportion of each test, respectively. The typical test results indicate that the random number sequences obtained from our QRNG can well pass all the NIST tests.

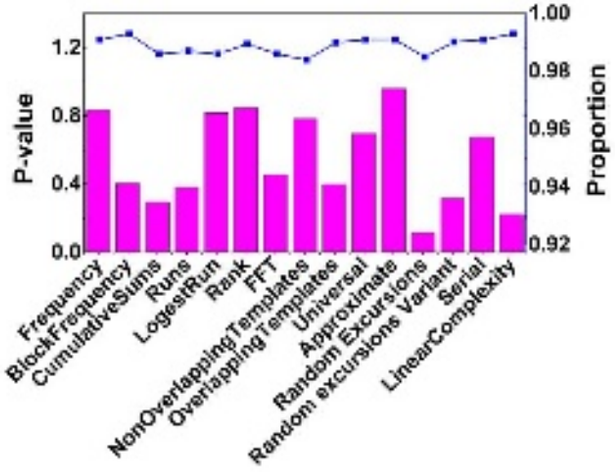


FIG. 8. NIST test results: P-value (left column) and proportion (right column). Note, the 15 test items are shown along the horizontal axis.

IV. DISCUSSIONS

We want to point that using parallel processing could greatly enhance the potential for further improving the QRNG rate. Obviously, one can easily extended the wide-spectra ASE signal into many independent random sources utilizing the spectrally-sliced technique. According to the requirements for parallel random number generation,[47] the spectrally sliced sub-entropy sources should be independent with each other. Here, we only take one case of them as an example to illustrate this point. Fig. 9(a) and Fig. 9(b) depict the RF spectra and the cross-correlation function (CCF) of the two different filtering channels outputs. Each filtering bandwidths are with a 0.6 nm, and their center wavelengths are $\lambda_1 = 1553.7$ nm, and $\lambda_2 = 1554.5$ nm, respectively. In our experiment, the time series of the two channels are simultaneously recorded at a sampling rate of 80 GSa/s for 0.2 ms, which is equivalent to a sample size of 16 Mbits. As shown in Fig. 9(a), all the RF spectra are very wide and flat. Such performance is beneficial for subsequent high-speed random bits extraction. From the CCF curve in Fig. 9(b), one can observe that the cross-correlation coefficient level is near zero. That indicates there is

no inter-channel correlation between the temporal waveforms of the two different spectral components in the SLD. This guarantee the independence of different subsequences at the source.

In our current experimental system, a single-channel filtering scheme is successfully implemented where we use only one filtering channel and consume no more than 0.6 nm. Considering that the 3-dB spectral width of the whole SLD is at least 55 nm, we believe that utilizing some extra filtering devices, the number of parallel wavelength channels can be increased to at least 90. In view of this point, our QRNG is expected to achieve an accumulative bit rates up to Tb/s.

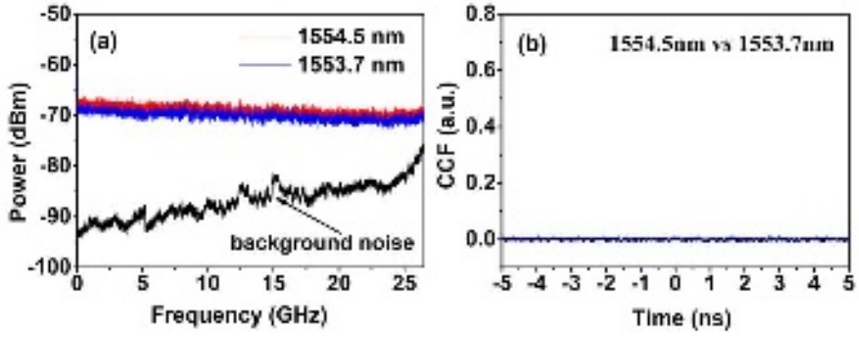


FIG. 9. (a) RF spectra and (b) the cross-correlation function (CCF) of two different filtering channels ASE noise signal, respectively.

Herein, we note that our proof-of-principle experiment uses discrete photonic and electronic components so that the whole system is relatively bulky. Fortunately, the integrated MLL and TOAD-based optical sampling gate have been reported with the advanced photonic integrated circuits (PICs) in recent years.[48-50] If the PIC techniques are introduced to design the QRNGs, our scheme may be monolithically integrated and thereby provide a highly compact device. One of our future works is to combine the PICs technology with quantum random bit generation.

V. CONCLUSIONS

In conclusion, we proposed and experimentally demonstrated a fast QRNG based on optically sampled ASE. In our proof-of-principle experiment, a low-complexity TOAD-based optical sampler is first introduced to perform the optical sampling function for fast quantum random number generation. Then, an 8-bit parallel comparator is used to digitize the obtained optically sampled pulses. Finally, by reserving 4 LSBs sampled at 10 GSa/s, a 40 Gb/s random bits sequence can be continuously obtained. Moreover, we also apply the min-entropy and the Toeplitz hashing to further evaluate and extract the quantum randomness. In contrast to electrical sampling, our approach can efficiently overcome the electronic jitter bottleneck. Thus, this proposal provides one way combining photonic signal processing with ultrafast quantum random numbers, which might also be a good alternative to conventional post-processing QRNGs employing electrical ADCs. In addition, with the rapid development of the PICs technology, it may allow us to explore more monolithically integrated QRNGs for future practical applications.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China under Grants (61775158, 61961136002, 61927811, U19A2076, 61705159, and 61805168); in part by the National Cryptography Development Fund under Grant (MMJJ20170127); in part by the China Postdoctoral Science Foundation under Grants (2018M630283, 2019T120197); in part by the Natural Science Foundation of Shanxi Province under Grant (201801D121015, 201901D211116); in part by the STCSM under Grant (SKLSFO2018-03); in part by 111 Project under Grant (D20031); in part by the Project of Key Laboratory of Radar Imaging and Microwave Photonics (Nanjing University of Aeronautics and Astronautics), Ministry of Education under Grant (RIMP2019002); in part by the Program for the Top Young Academic Leaders of High Learning Institutions of Shanxi; in part by the Fund for Shanxi "1331 Project" Key Innovative Research Team.

DATA AVAILABILITY

The data that supports the findings of this study are available within the article [and its supplementary material].

REFERENCE

1. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum Random Number Generators," Rev. Mod. Phys. **89**(1), 015004 (2017).
2. M. N. Bera, A. Acín, M. Kus, M. W. Mitchell, and M. Lewenstein, "Ran-domness in Quantum Mechanics: Philosophy, Physics and Technology," Rep. Prog. Phys. **80**(12), 124001 (2017).
3. B. Qi, Y. M. Chi, H. K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single mode laser," Opt. Lett. **35**(3), 312-314 (2010).
4. X. G. Zhang, Y. Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J. W. Pan, "68 Gbps quantum random number generation by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**(6), 063105 (2015).
5. J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. J. Xu, and H. Guo, "5.4 Gbps real time quantum random number generator with simple implementation," Opt. Express **24**(24), 27475-27481 (2016).
6. H. Q. Ma, Y. J. Xie, and L. A. Wu, "Random number generation based on the time of arrival of single photons," Appl. Opt. **44**(36), 7760-7763 (2005).
7. M. Fürst, H. Weier, S. Nauerth, S. Nauerth, D. G. Marangon, C. Kurtsiefer and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**(12), 13029-13037 (2010).
8. M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H. J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," Appl. Phys. Lett. **98**(17), 171105 (2011).
9. Y. Q. Nie, H. F. Zhang, Z. Zhang, J. Wang, X. F. Ma, J. Zhang, and J. W. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference," Appl. Phys. Lett. **104**(5), 051110 (2014).
10. Q. R. Yan, B. S. Zhao, Q. H. Liao, and N. R Zhou, "Multi-bit quantum random number generation by measuring positions of arrival photons," Rev. Sci. Instrum. **85**(10), 103116 (2014).
11. M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan. D. A. Ritchie, and A. J. Shields, "Efficient and robust quantum random number generation by photon number detection," Appl. Phys. Lett. **107**(7), 175-179 (2015).

12. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. G. Mauerer, U. L. Andersen, C. Marquardtand, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**(10), 711-715 (2010).
13. 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**(21), 20665-20672 (2011).
14. C. R. S. Williams, J. C. Salevan, X. W. Li, R. Roy, and T. E. Murph, "Fast physical random number generator using amplified spontaneous emission," Opt. Express **18**(23), 23584-23597 (2010).
15. L. Li, A. B. Wang, P. Li, H. Xu, L. S. Wang, and Y. C. Wang, "Random Bit Generator Using Delayed Self-Difference of Filtered Amplified Spontaneous Emission," IEEE Photon. J. **6**(1), 1-9 (2014).
16. S. H. Wei, J. Yang, F. Fan, W. Huang, D. S. Li, and B. J. Xu, "Compact quantum random number generator based on superluminescent light-emitting diodes," Rev. Sci. Instrum. **88**(12), 123115 (2017).
17. T. Tomaru, "Continuous-variable random-number generation from an amplified spontaneous emission light source," Appl. Optics. **59**(10), 3109-3118 (2020).
18. X. W. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a super-luminescent LED," Opt. Lett. **36**(6), 1020-1022 (2011).
19. W. Wei, G. D. Xie, A. H. Dang, and H. Guo, "High-Speed and Bias-Free Optical Random Number Generator," IEEE Photon. Technol. Lett. **24**(6), 437-439 (2012).
20. A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-Tb/s Physical Random Bit Generators Based on Direct Detection of Amplified Spontaneous Emission Signals," J. Lightwave Technol. **30**(9), 1329-1334 (2012).
21. T. M. Souders, D. R. Flach, C. Hagwood, and G. L. Yang, "The effects of timing jitter in sampling systems," IEEE T. Instru. Meas. **39**(1), 80-85 (1990).
22. A. Mahjoubfar, D. V. Churkin, S. Barland, N. Broderick, S. K. Turitsyn, and B. Jalali, "Time stretch and its applications," Nat. Photonics. **11**(6), 341-351 (2017).
23. G. C. Valley, "Photonic analog-to-digital converters," Opt. Express **15**(5), 1955-1982 (2007).
24. A. Khilo et al., "Photonic ADC: Overcoming the bottleneck of electronic jitter," Opt. Express **20**(4), 4454-4467 (2012).
25. P. Li, Y. Y. Sun, X. L. Liu, X. G. Yi, J. G. Zhang, X. M. Guo, Y. Guo, and Y. C. Wang, "Fully photonics-based physical random bit generator," Opt. Lett. **41**(14), 3347-3350 (2016).
26. E. W. Jacobs et al., "Optically clocked track-and-hold for high-speed high-resolution analog-to-digital conversion," in International Topical Meeting on Microwave Photonics, Ogunquit, ME, 190-192 (2004).
27. N. Yamada, H. Ohta, and S. Nogiwa, "Jitter-free optical sampling system using passively modelocked fiber laser," Electron. Lett. **38**(18), 1044-1045 (2002).
28. X. F. Ma, X. Yuan, X; Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," NPJ. Quantum. Inform. **2**, 16021, 2016.
29. S. H. Sun, and F. Xu, "Experimental study of a quantum random-number generator based on two independent lasers," Phys. Rev. A. **96**(6), 062314 (2017).
30. Y. Q. Nie, L. L. Huang, Y. Liu, F. Payne, J. Zhang, and J. W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**(6), 062315 (2015).
31. Q. Zhang, D. H. Kong, Y. B. Wang, H. X. Zou, and H. Chang, "Dual-entropy-source quantum random number generation based on spontaneous emission," Opt. Lett. **45**(2), 304-307 (2020).
32. L. L. Huang, and H. Y. Zhou, "Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection," J. Opt. Soc. Am. B. **36**(3), B130-B136 (2019).

33. J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma. P. K. Lam, and T. Symul2013, "Maximization of Extractable Randomness in a Quantum Random-Number Generator," Phys. Rev. Appl. **3**(5), 054004 (2015).

34. X. F. Ma, F. H. Xu, H. Xu, X. Q. Tan, B. Qi, and H. K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A. **87**(6), 062327 (2013).

35. A. Bogoni, F. Ponzini, M. Scaffardi, P. Ghelfi, and L. Poti, "New Optical Sampler Based on TOAD and Data Postprocessing for Subpicosecond Pulse Resolution," IEEE J. Sel. Top. Quantum Electron. **10**(1), 186-194 (2004).

36. D. K. Gayen, and J. N. Roy, "All-optical arithmetic unit with the help of terahertz-optical-asymmetric-demultiplexer-based tree architecture," Appl. Optics **47**(7),933-943 (2008).

37. P. Li, L. Jiang, J. G. Zhang, J. Z. Zhang, and Y. C. Wang, "Low-Complexity TOAD-Based All-Optical Sampling Gate with Ultralow Switching Energy and High Linearity," IEEE Photonics. J. **7**(4), 1-8 (2015).

38. F. H. Xu, B. Qi, X. F. Ma, H. Xu, H. X. Zheng, and H. K Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**(11), 12366-12377 (2012).

39. L. Trevisan, "Extractors and pseudorandom generators," J. ACM. **48** (4), 860–879 (2001).

40. J. Yang, F. Fan, J. L. Liu, Q. Su, Y. Li, W. Huang, and B. J. Xu, "Randomness quantifcation for quantum random number generation based on detection of amplifed spontaneous emission noise," Quantum Sci. Technol. **6**, 015002 (2020).

41. X. Yuan, Q. Zhao, D. Girolami, and X. F. Ma, "Quantum Coherence and Intrinsic Randomness," Adv. Quantum Technol. **2** (11), 1900053 (2019).

42. H. Y. Zhou, P. Zeng, M. Razavi, and X. F. Ma, "Randomness quantification of coherent detection," Phys. Rev. A. **98** (4), 042321 (2018).

43. Q. Zhang, X. W. Deng, C. X. Tian, and X. L. Su, "Quantum random number generator based on twin beams," Opt. Lett. **42** (5), 895-898 (2017).

44. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side Information," IEEE Trans. Inf. Theory. **57** (8), 5524-5535 (2011).

45. A. De, C. Portmann, T. Vidick, and R. Renner, "Toeplitz's extractor in the presence of quantum side information," IEEE Trans. Inf. Theory. **41** (4), 915-940 (2012).

46. See http://csrc.nist.gov/groups/ST/toolkit/rng/index.html for information about the NIST test suite.

47. P. Li, K. Y. Li, X. M. Guo, Y. Q. Guo. Y. M. Liu, B. J. Xu, A. Bogris, K. A. Shore, and Y. C. Wang, "Parallel optical random bit generator," Opt. Lett. **44**(10), 2446-2449 (2019).

48. L. P. Hou, M. Haji and J. H. Marsh, "Monolithic Mode-Locked Laser With an Integrated Optical Amplifier for Low-Noise and High-Power Operation," IEEE J. Sel. Top. Quantum Electron. **19** (4), 1100808 (2013).

49. I. Glesk, R. J. Runser, and P. R. Prucnal, "New generation of devices for all-optical communications," Acta. Phys. Slovaca. **51** (2), 151-162 (2001).

50. G. K. Maity, T. Chattopadhyay, D. K. Gayen, C. Taraphdar, A. K. Maiti, S. P. Maity, and J. N. Roy, "All-optical binary flip-flop with the help of Terahertz Optical Asymmetric Demultiplexer," Nat. Comput. **9** (4), 903-916 (2010).

Figure Legends

FIG. 1. Schematic diagram of the proposed post-processing-free fast QRNG based on optically sampled ASE: (a) ASE source, (b) Optical sampler, and (c) 8-bit parallel comparator. SLD, super-luminescent diode; EDFA, Er-doped fiber amplifier; BPF1, BPF2, optical band-pass filters; MLL, mode-locked laser; WDM, wavelength division multiplexer coupler; SOA, semiconductor optical amplifier; PC1, PC2 polarization controllers; 50:50, 50:50 optical coupler; TOAD, terahertz optical asymmetric demultiplexer; ISO, optical isolator; PD, photodetector; LSB, least significant bit; MSB, most significant bit.

FIG. 2. Schematic Characteristics of the filtered ASE. (a) The optical spectra of the SLD (the black line) and the spectrally-sliced channel (the blue line). (b) The RF spectrum of the filtered ASE (the blue line) and the electrical background noise (the black line). (c) The temporal waveform and the amplitude distribution of the filtered ASE and the classical noise (the red line is the Gaussian fitted curve). (d) The autocorrelation trace of the filtered ASE temporal waveforms.

FIG. 3. Optical sampling characteristics. (a) Continuous-time ASE noise temporal waveforms to be sampled and (b) discrete-time ASE pulses temporal waveforms after the optical sampling procedure.

FIG. 4. Linearity evaluation of the TOAD-based all-optical sampler.

FIG. 5. Statistical distribution of the ASE noise amplitudes before and after optical sampling with the TOAD.

FIG. 6. Quantization principle of the optically sampled ASE pulses train (take a 3-bit quantization as an example).

Fig. 7. (a) Bias |e[N]| versus the sample size of the generated 40 Gb/s random bit stream; The red line in (a) is its three-standard-deviation line, $3\sigma_e = (3N^{-1/2})/2$ where n = 1, 2, 3, …, 16Mbits. (b) Autocorrelation coefficient C[K] as a function of the delay bit K for a 16×10^6 bit.

FIG. 8. NIST test results: P-value (left column) and proportion (right column). Note, the 15 test items are shown along the horizontal axis.

FIG. 9. (a) RF spectra and (b) the cross-correlation function (CCF) of two different filtering channels ASE noise signal, respectively.

Figures

Fig.1

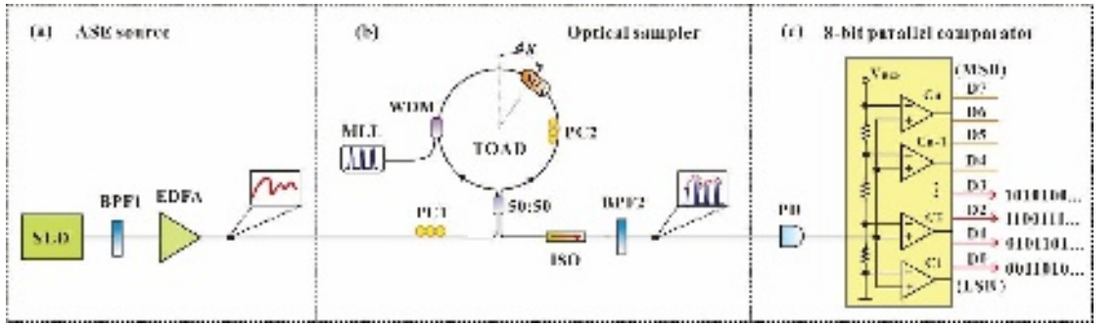


Fig.2

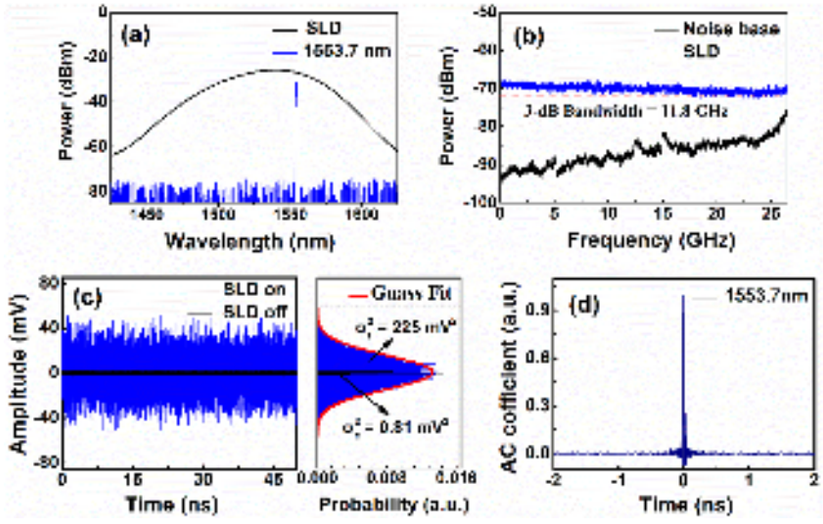


Fig.3

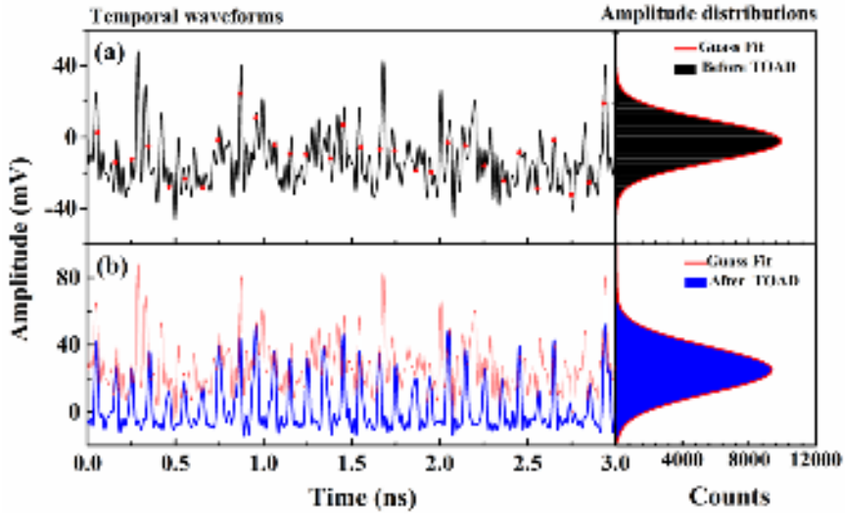


Fig.4

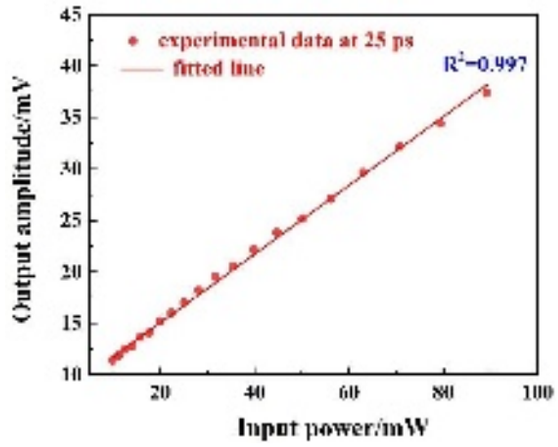


Fig.5

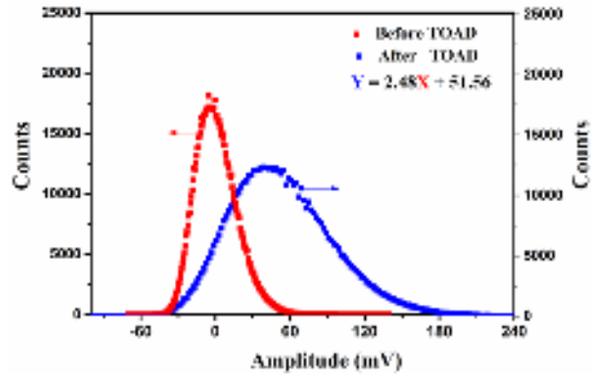


Fig.6

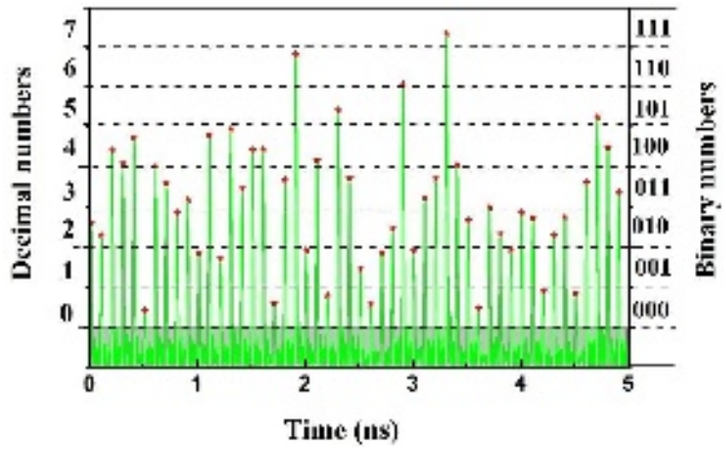


Fig.7

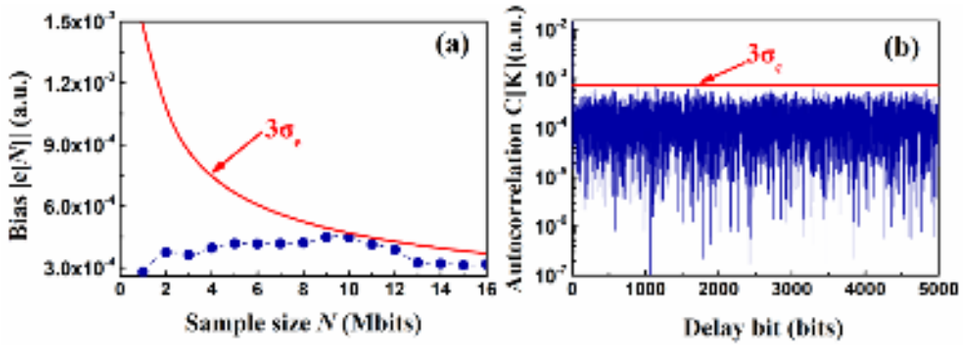


Fig.8

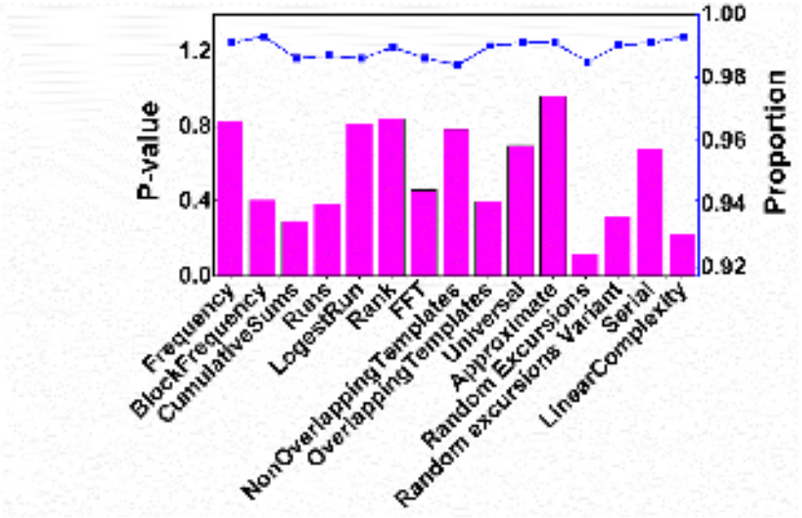
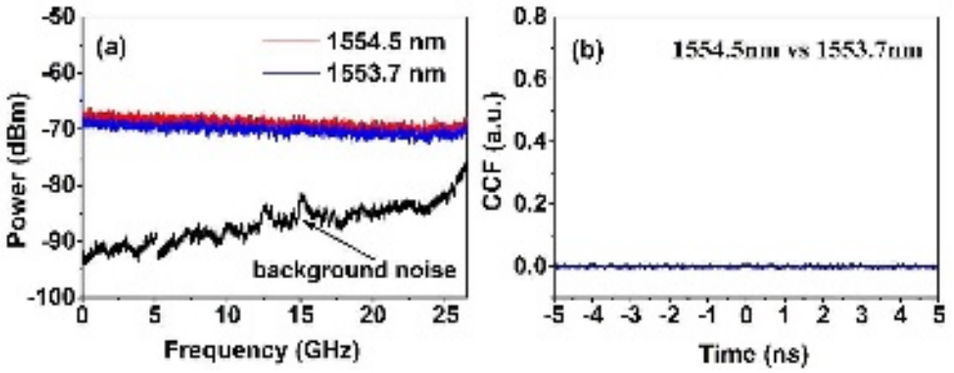
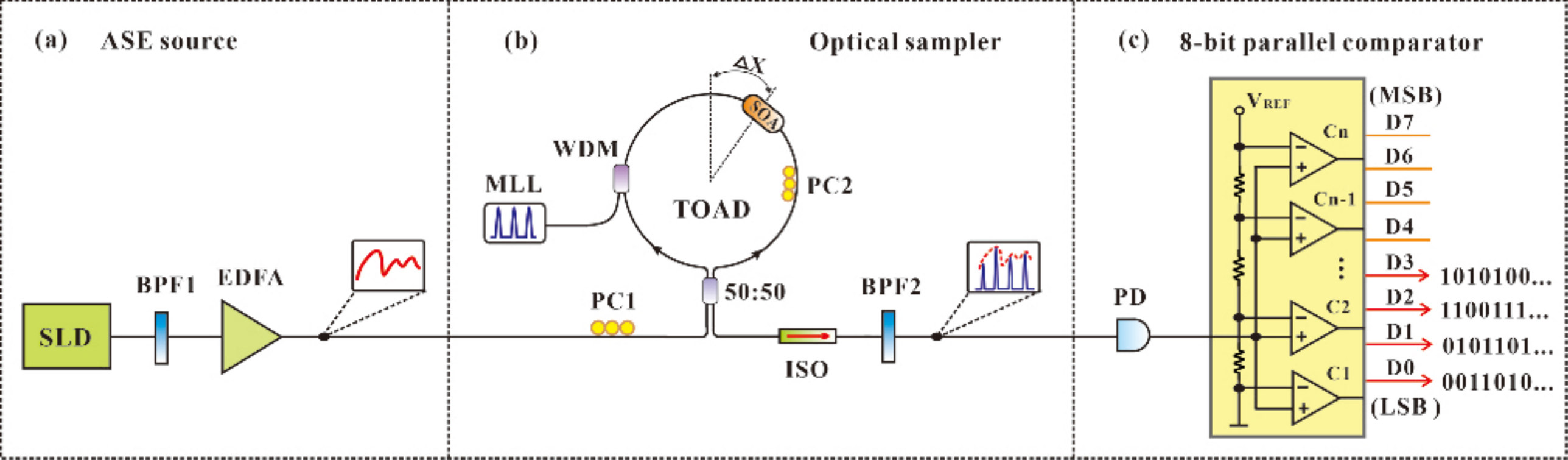
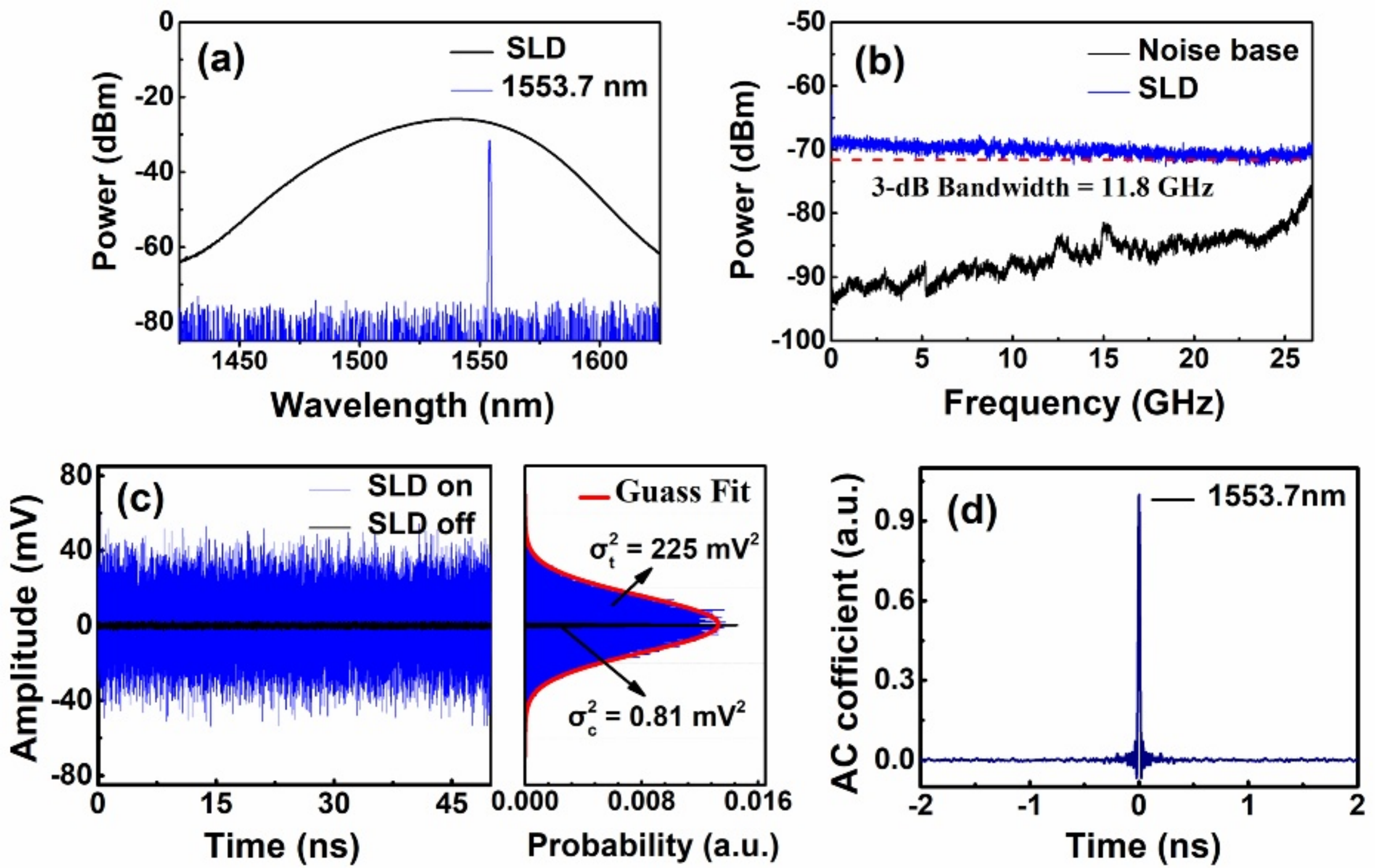
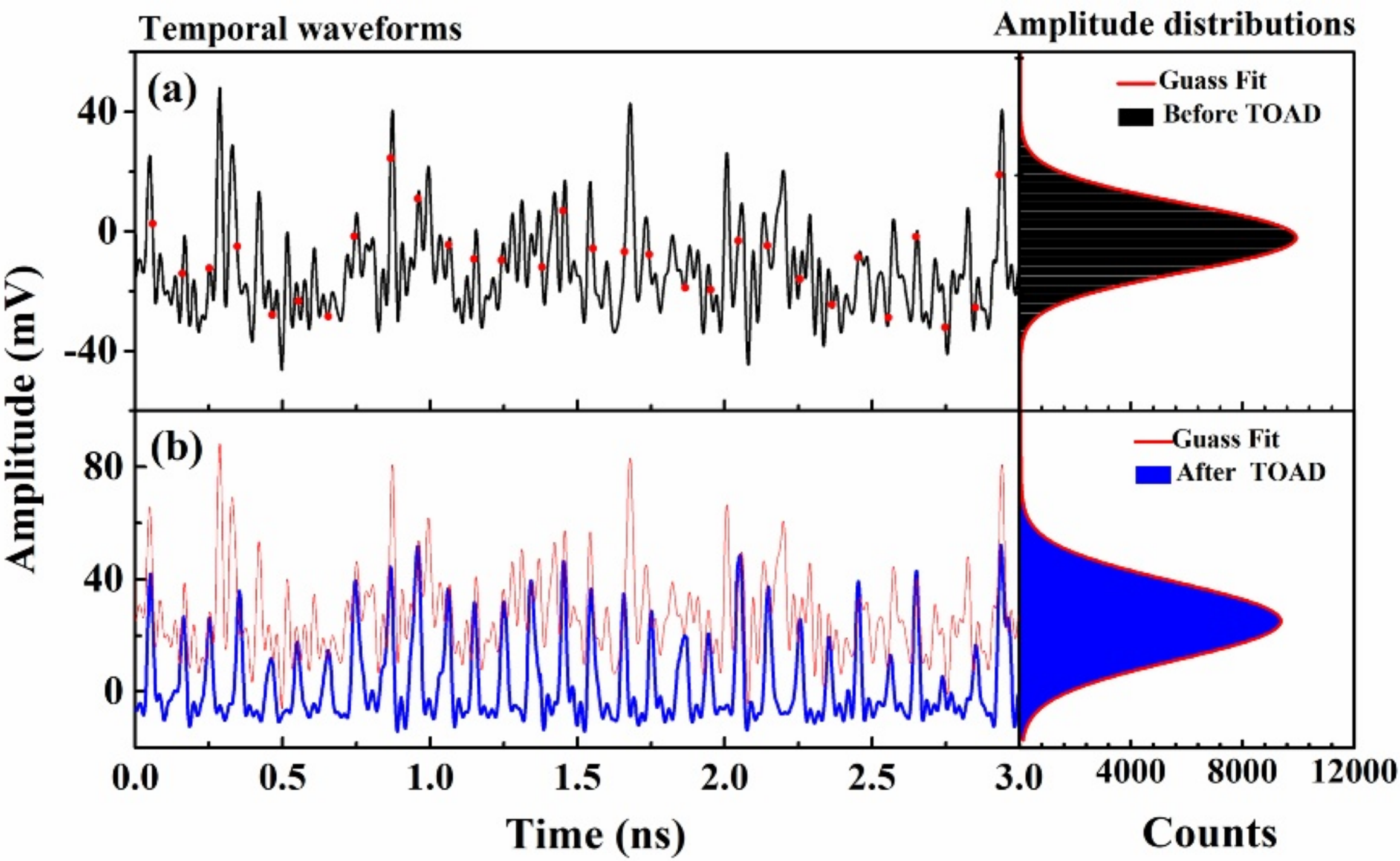


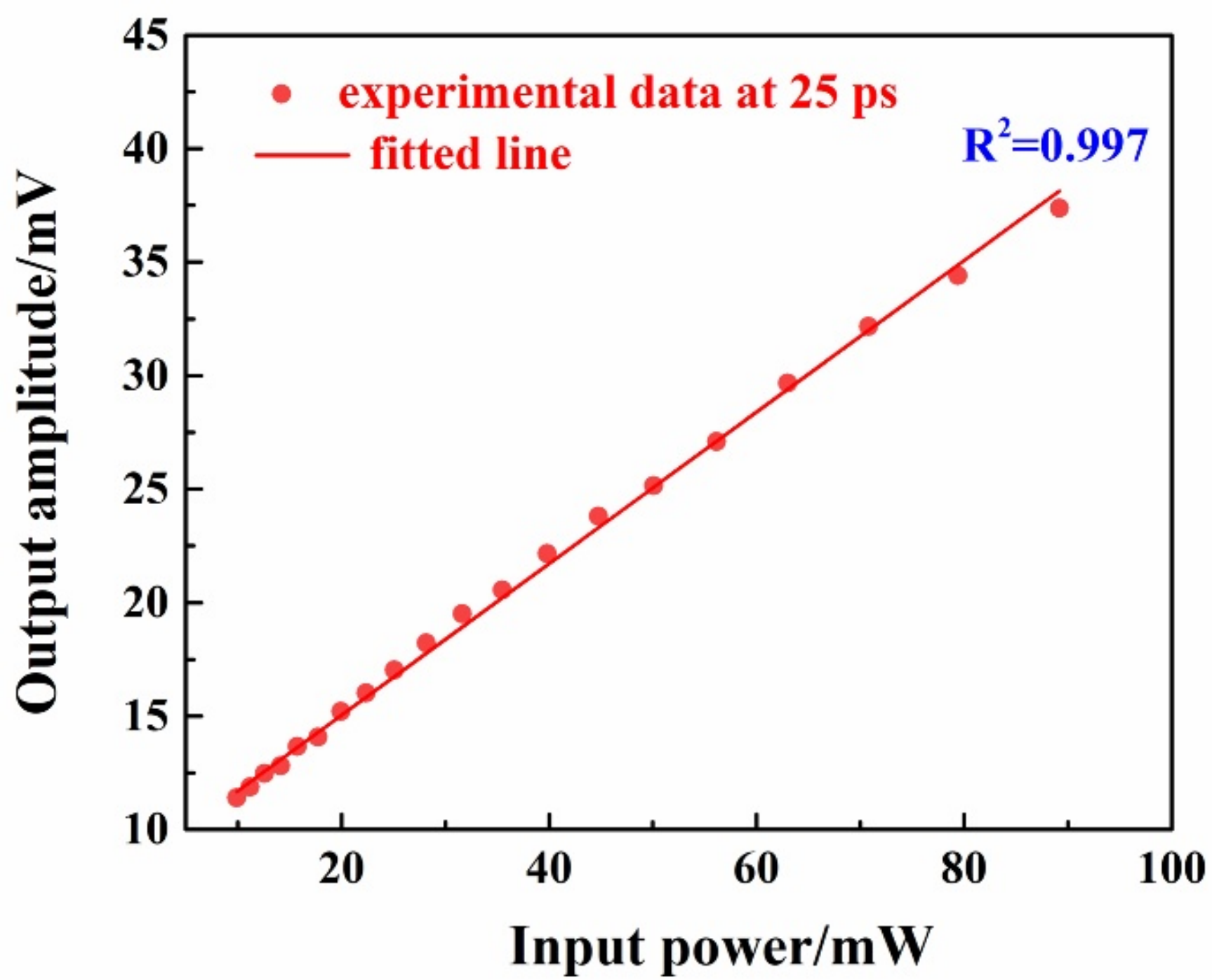
Fig.9

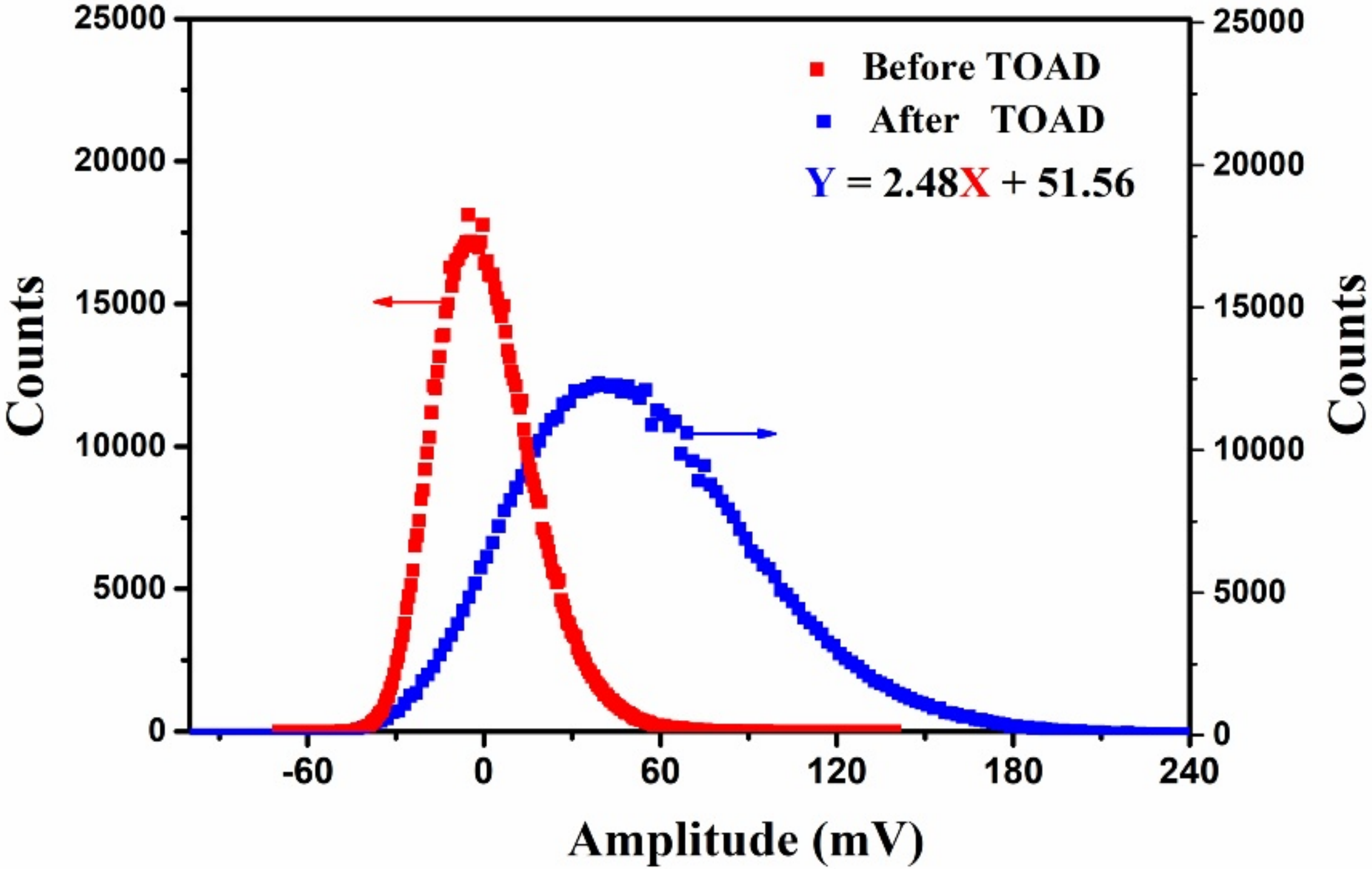


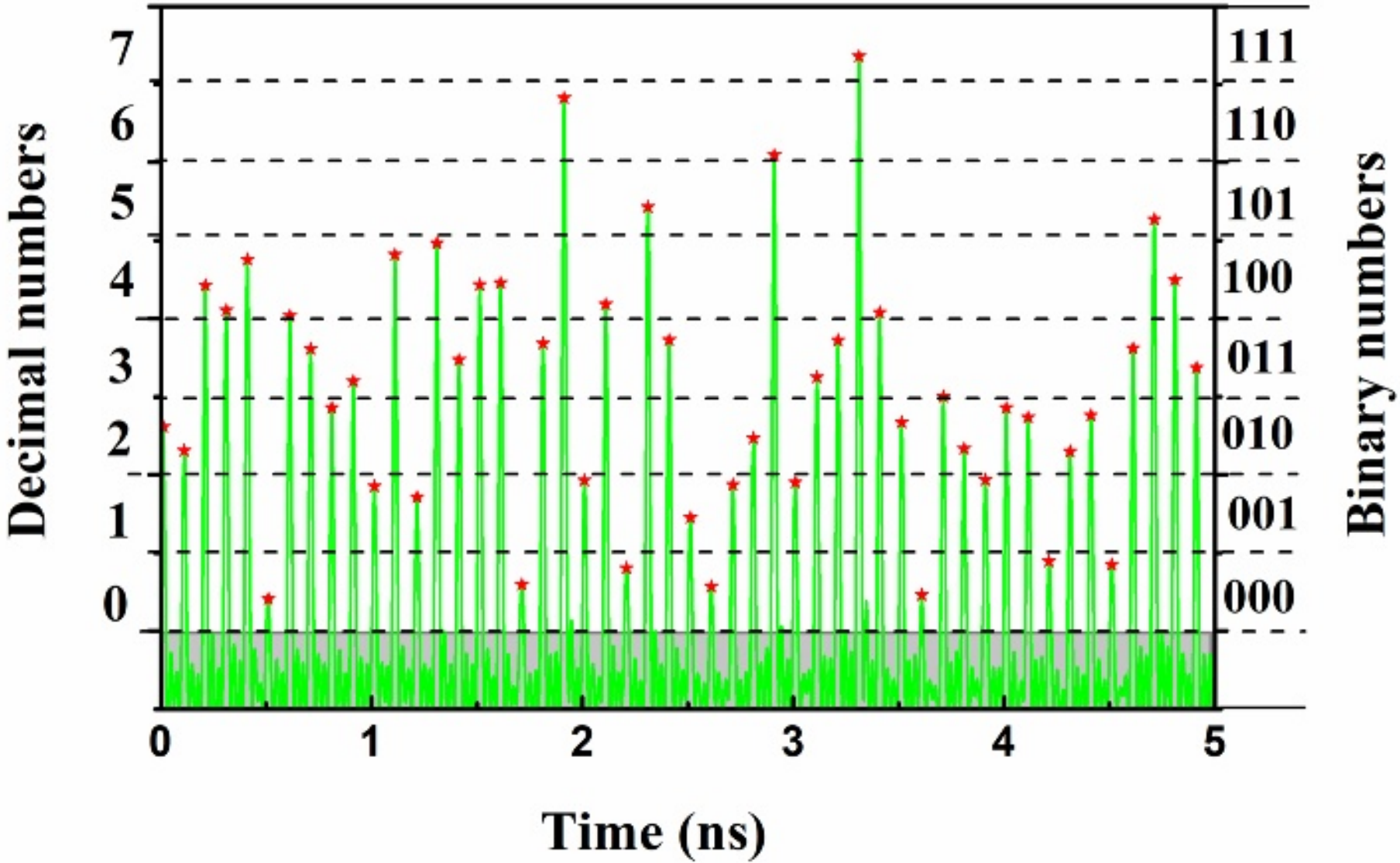

(a) ASE source
SLD
BPF1
EDFA
(b) Optical sampler
4X
SOA
WDM
MLL
TOAD
PC2
PC1
50:50
ISO
BPF2
PD
(c) 8-bit parallel comparator
VREF
Cn
Cn-1
C2
C1
(MSB)
D7
D6
D5
D4
D3
D2
D1
D0
(LSB)
1010100...
1100111...
0101101...
0011010...

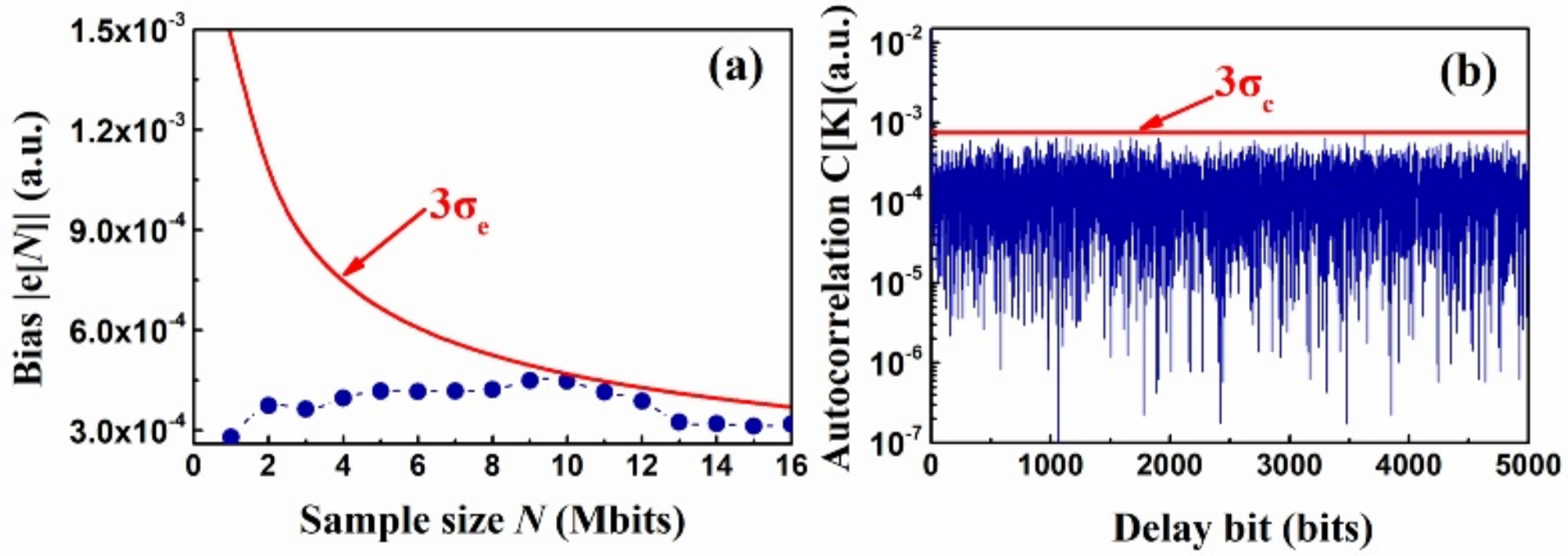

(a)
SLD
1553.7 nm
Power (dBm)
Wavelength (nm)
(b)
Noise base
SLD
3-dB Bandwidth = 11.8 GHz
Power (dBm)
Frequency (GHz)
(c)
SLD on
SLD off
Amplitude (mV)
Time (ns)
Guass Fit
σ_t^2 = 225 mV^2
σ_c^2 = 0.81 mV^2
Probability (a.u.)
(d)
1553.7nm
AC cofficient (a.u.)
Time (ns)

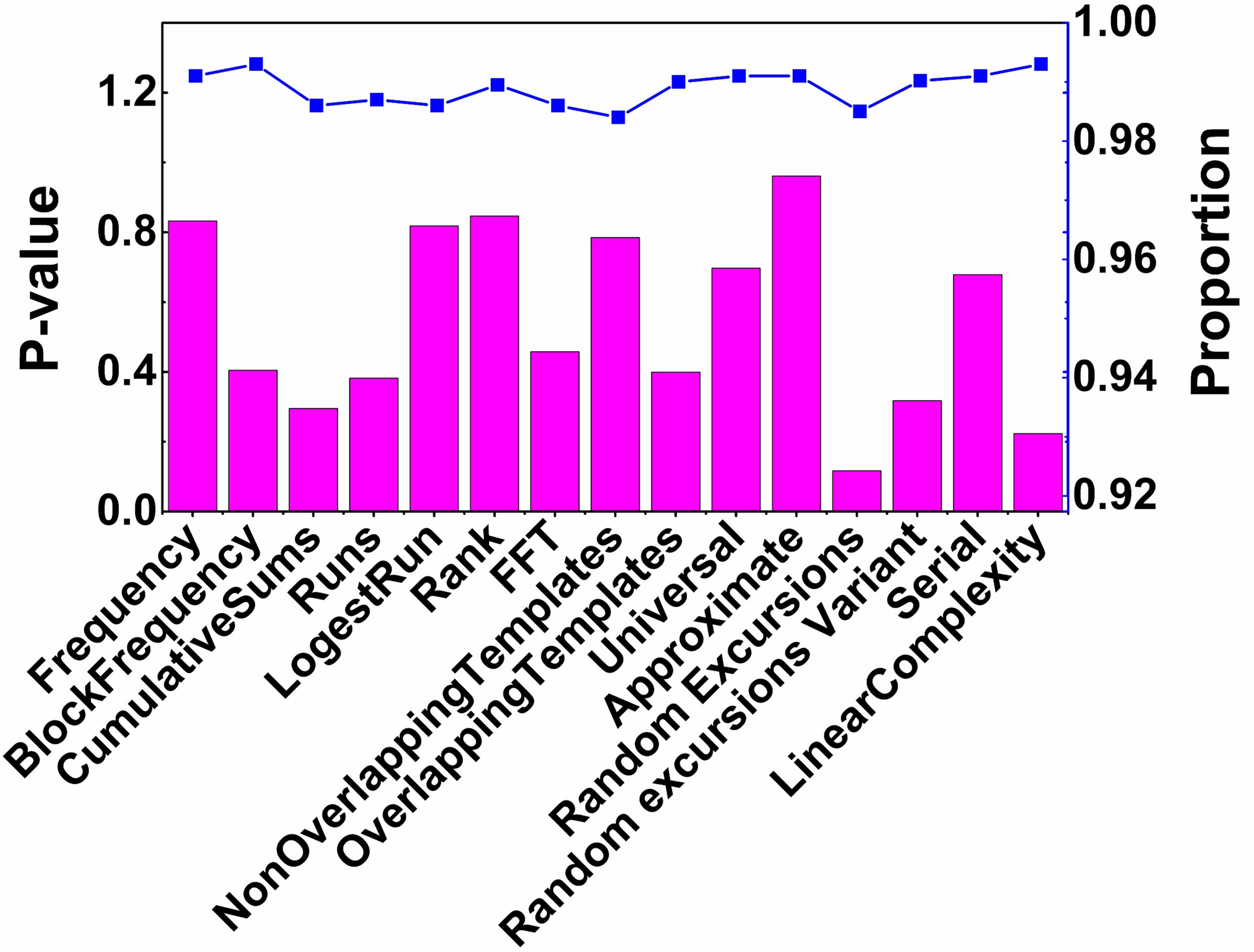

Temporal waveforms
Amplitude distributions
(a)
(b)
Guass Fit
Before TOAD
Guass Fit
After TOAD
Amplitude (mV)
40
0
-40
80
40
0
0.0
0.5
1.0
1.5
2.0
2.5
3.0
4000
8000
12000
Time (ns)
Counts

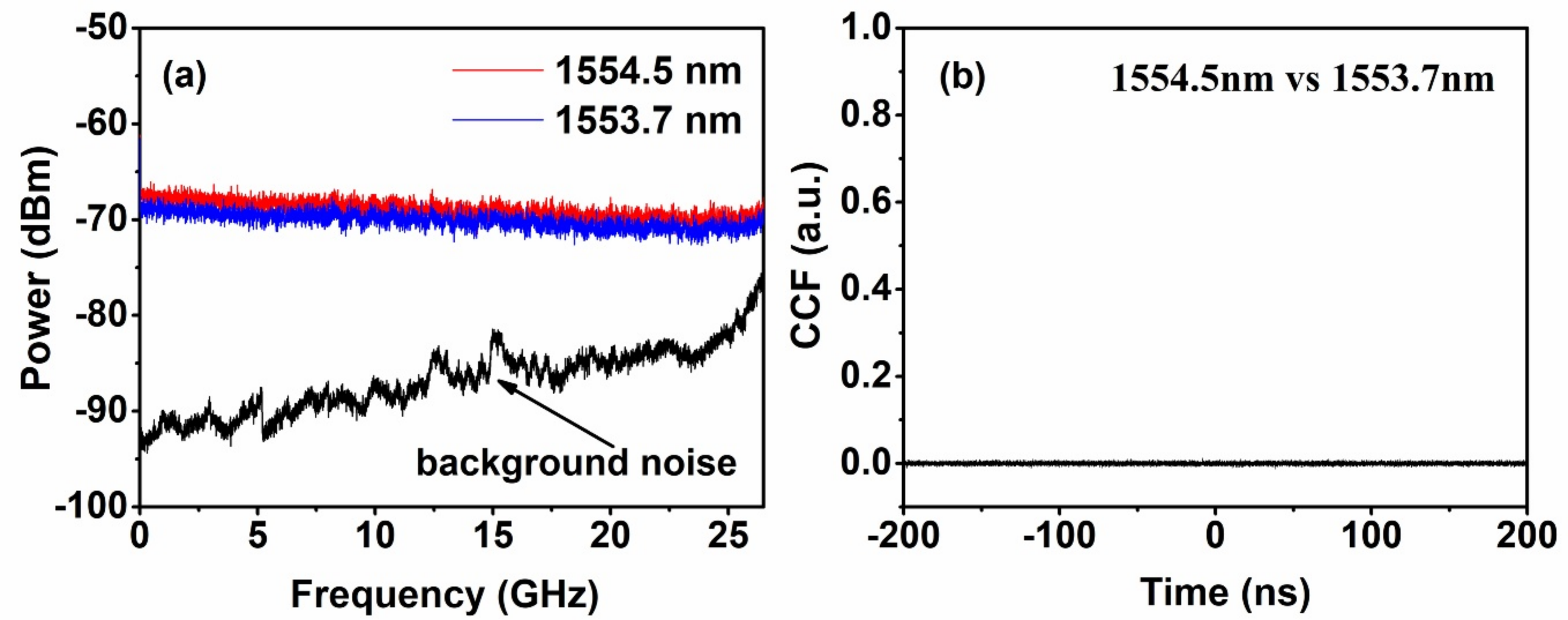

experimental data at 25 ps
fitted line
R²=0.997
Output amplitude/mV
Input power/mW
45
40
35
30
25
20
15
10
20
40
60
80
100


Before TOAD
After TOAD
Y = 2.48X + 51.56
Counts
Counts
Amplitude (mV)
25000
20000
15000
10000
5000
0
-60
0
60
120
180
240


Decimal numbers
7
6
5
4
3
2
1
0
111
110
101
100
011
010
001
000
Binary numbers
0
1
2
3
4
5
Time (ns)


(a)
1.5x10^-3
1.2x10^-3
9.0x10^-4
6.0x10^-4
3.0x10^-4
Bias |e[N]| (a.u.)
3σe
0
2
4
6
8
10
12
14
16
Sample size N (Mbits)
(b)
3σc
10^-2
10^-3
10^-4
10^-5
10^-6
10^-7
Autocorrelation C[K](a.u.)
0
1000
2000
3000
4000
5000
Delay bit (bits)


P-value
Proportion
0.0
0.4
0.8
1.2
0.92
0.94
0.96
0.98
1.00
Frequency
BlockFrequency
CumulativeSums
Runs
LogestRun
Rank
FFT
NonOverlappingTemplates
OverlappingTemplates
Universal
Approximate
Random Excursions
Random excursions Variant
Serial
LinearComplexity


(a)
1554.5 nm
1553.7 nm
background noise
Power (dBm)
-50
-60
-70
-80
-90
-100
0
5
10
15
20
25
Frequency (GHz)
(b)
1554.5nm vs 1553.7nm
CCF (a.u.)
1.0
0.8
0.6
0.4
0.2
0.0
-200
-100
0
100
200
Time (ns)