Research Article

Nano Research
2022, 15(5): 4448–4456

ISSN 1998-0124 CN 11-5974/O4
https://doi.org/10.1007/s12274-022-4109-9

A flexible and stretchable bionic true random number generator

Yongbiao Wan[1,2,§], Kun Chen[1,2,§], Feng Huang[1,2], Pidong Wang[1,2], Xiao Leng[1,2], Dong Li[1,2], Jianbin Kang[1,2], Zhiguang Qiu[3] (✉), and Yao Yao[1,2] (✉)

[1] *Microsystem and Terahertz Research Center, China Academy of Engineering Physics, Chengdu 610200, China*
[2] *Institute of Electronic Engineering, China Academy of Engineering Physics, Mianyang 621999, China*
[3] *School of Electronics and Information Technology, State Key Lab of Opto-Electronic Materials & Technologies, Guangdong Province Key Lab of Display Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, China*
[§] *Yongbiao Wan and Kun Chen contributed equally to this work.*

Received: 15 November 2021 / **Revised:** 20 December 2021 / **Accepted:** 24 December 2021

ABSTRACT

The volume of securely encrypted data transmission increases continuously in modern society with all things connected. Towards this end, true random numbers generated from physical sources are highly required for guaranteeing security of encryption and decryption schemes for exchanging sensitive information. However, majority of true random number generators (TRNGs) are mechanically rigid, and thus cannot be compatibly integrated with some specific flexible platforms. Herein, we present a flexible and stretchable bionic TRNG inspired by the uniqueness and randomness of biological architectures. The flexible TRNG film is molded from the surface microstructures of natural plants (e.g., ginkgo leaf) via a simple, low-cost, and environmentally friendly manufacturing process. In our proof-of-principle experiment, the TRNG exhibits a fast generation speed of up to 1.04 Gbit/s, in which random numbers are fully extracted from laser speckle patterns with a high extraction rate of 72%. Significantly, the resulting random bit streams successfully pass all randomness test suites including NIST, TestU01, and DIEHARDER. Even after 10,000 times cyclic stretching or bending tests, or during temperature shock (−25–80 °C), the bionic TRNG still reveals robust mechanical reliability and thermal stability. Such a flexible TRNG shows a promising potential in information security of emerging flexible networked electronics.

KEYWORDS

random number generator, flexible electronics, polydimethylsiloxane (PDMS), bionic microstructure, information security

1 Introduction

Striving towards the advances of artificial intelligence, big data, and the Internet of Things, the proliferation of cyber-physical devices, such as embedded flexible electronic systems and wearable technologies, has brought unprecedented levels of data collection, analysis, and exchange [1–5]. As more interconnected devices across the globe are developed to manage private and sensitive data, information security has been one of the most important concerns, showing an urgent demand for robust security primitives. In this regard, various components of security primitives have been proposed, such as asymmetric ciphers, symmetric ciphers, physical unclonable function, and random number generation [6–10]. Among these, data encryption using random numbers (e.g., one-time pad [11]) is one of the most effective approaches to guarantee the secure communication between devices, owing to the advantages of unpredictability, unbiasedness, and superior statistical characteristics [12]. In particular, indispensable encryption and decryption processes require random numbers with expected statistical randomness and robust security, which can effectively prevent malicious persons or organizations from accessing data during its storage and transmission.

Two methods are generally used to produce the required random numbers: true random number generator (TRNG) based on physical entropy sources and pseudo random number generator (PRNG) which relies on software algorithms. Whereas PRNG can be attacked by an exhaustive method since it is a deterministic algorithm expanding a fixed number "seed" into a long sequence [13]. Accordingly, with the dramatic increase of computational speed and decoding capacity, conventional PRNGs are becoming increasingly insecure. For instance, machine learning attacks are now able to crack and predict the output from the traditional pseudo random algorithms [14]. If random numbers are not credible, the encrypted information could be stolen by the listener-in, which exposes the vulnerability of present state-of-the-art information security systems. In contrast, physical TRNGs exploit some unpredictable or, at least, difficult to predict physical process and use the outputs to produce a bits sequence that can be truly random[12], thus enabling superior reliability for data encryption and other applications, such as cybersecurity, stochastic modeling, lottery, or games of chance [15–17]. Up to date, a series of TRNGs based on different physical sources with different working mechanisms has been investigated to generate considerable random numbers in lieu of conventional pseudo random numbers, such as random telegraph noise (RTN) based on memristors [18–22], thin-film transistor [23–25], and triboelectric generator [26, 27], laser chaos [28–30], photonic

Address correspondence to Zhiguang Qiu, zhiguangqiu88@gmail.com; Yao Yao, yaoyao_mtrc@caep.cn

integrated chip [31], quantum entropy sources [32–35], bichromatic laser dye [36], crystallization robot [37], DNA synthesis [38], and so forth. However, majority of aforementioned existing TRNG implementations rely on rigid platforms and expensive complicated manufacturing crafts, which cannot compatibly adapt the portable networked devices and systems since emerging wearable technologies typically demand low-cost and mechanically flexible security hardware components. Although Rojas et al. [23] conceptually proposed a so-called flexible thin-film transistor-based TRNG with a static random access memory structure made by single-walled carbon nanotubes and silicon technology, actually the random performances of the TRNG under mechanically flexible state were not investigated, and the structure of this TRNG has limit flexibility that cannot be stretched or drastically bent. For this reason, more efficient, economical, flexible, and even stretchable TRNG alternative approaches are imperative for filling up the research gap of information security toward emerging flexible hardware systems.

Life can feel stochastic in many cases, and we often try to create order from randomness. Sometimes, however, randomness is worth pursuing, where it contains valuable resources for TRNGs manufacture. Herein, we demonstrate a flexible and stretchable bionic TRNG inspired from the uniqueness and randomness of natural biological architectures. The bionic TRNG film is templated by the surface micro-nanostructure of natural plants (e.g., ginkgo leaf) via a simple, inexpensive, green, and environmentally friendly manufacturing craft. Upon illuminations of the modulated laser lights, the flexible TRNG could produce a series of transmitted speckle patterns for random numbers generation. Notably, the flexible TRNG exhibits a fast generation speed of 1.04 Gbit/s with a high extraction rate of 72%, and superior flexibility that can be stretched to 200% strain. In addition, resulting random numbers possess expected statistical characteristics, and pass all randomness test suites including NIST, TestU01, and DIEHARDER. After 10,000 times cyclic stretching with 50% strain or bending (bending radius, 5 mm) tests, or even during temperature shock (−25–80 °C), the flexible TRNG could still successfully produce credible random numbers, showing a desirable mechanical robustness. More remarkably, the bionic TRNG could be operated as a wearable wristband or a flexible label attached to a curved entity under diversified scenarios. Given the advantages of the flexible TRNG, a concept of encrypted communication between networked components of a deep-sea exploration system is proposed. We believe that such a flexible and stretchable bionic TRNG will open a new pathway for safeguarding future information security of flexible networked electronics.

2 Results and discussion

2.1 Concept and fabrication

Randomness is a fundamental feature of nature [39]. In other words, there are no two "leaves" that are exactly the same in the world, and each of biological architectures is unique. Nature has been constantly offering many valuable functional materials and inspiration to human beings [40–42]. Significantly, many surface microstructures of natural plant tissues can be templated to fabricate bionic structural film, which has been widely used in flexible electronics [43]. Inspired by this, we propose the concept of a flexible and stretchable bionic TRNG as depicted in Fig. 1. The bionic TRNG film was made via a simple and low-cost soft lithography method [44]. In craft processes, we choose polydimethylsiloxane (PDMS) as mould printing material owing to its intriguing properties such as simple processing, mechanical robustness, thermal stability, high transparency, biological compatibility, and chemical inertness [43]. Firstly, the uncured PDMS solution is uniformly coated onto the ginkgo leaf template. After heat curing and peeling off, the flexible bionic TRNG film with negative surface microstructures of the ginkgo leaf is obtained. Figure S1 in the Electronic Supplementary Material (ESM) shows the detailed light path diagram of experimental setups. A collimated and expanded laser beam with a central wavelength of 638 nm goes through the beam splitter and illuminates onto a phase-only liquid crystal spatial light modulator (SLM), where pseudo random patterns (see Fig. S2 in the ESM) are loaded to create challenges by modulating the laser beam wavefront through randomly setting each pixel's value. After penetrating through the lens and theiris, the input laser challenge is projected onto the bionic TRNG film. Behind the TRNG film, the speckle patterns are detected using a charge-coupled device (CCD) camera. By filtering with the in-house-developed post-processing algorithm, the speckle patterns could be converted into binary numbers as shown in the schematic computer of Fig. 1. Finally, the extracted random numbers are assessed by randomness test suites. Such a flexible and stretchable bionic TRNG shows a promising potential in the application of data encryption between networked wearable electronics as depicted in the left section of Fig. 1.

Figure 2(a) shows a top-view scanning electron microscope (SEM) image of the ginkgo leaf template, where there are long convex structures like continuous mountains on the surface of the sample. The distance between two mountain tops is about 400 μm. In addition, more detailed dense ellipsoidal small bumps are randomly distributed in convex mountain microstructures.

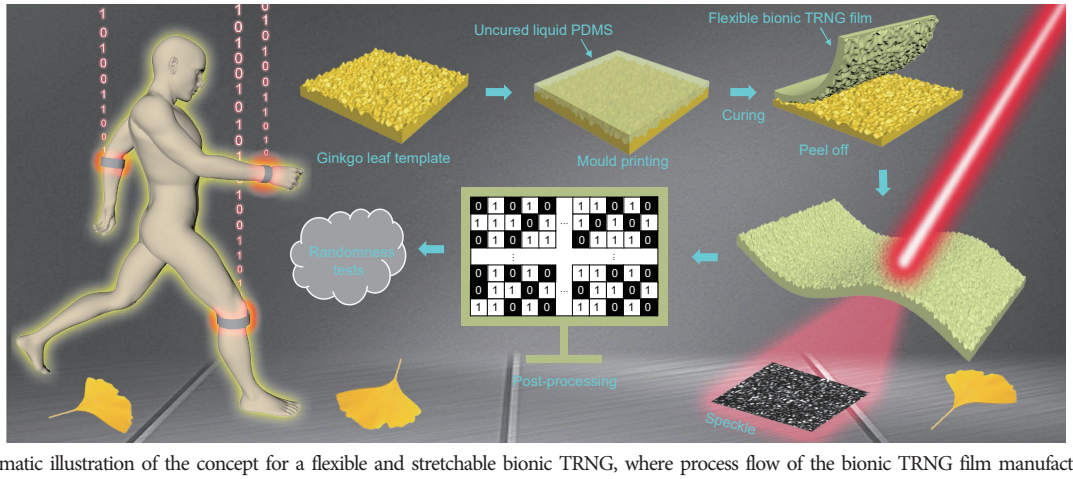

Figure 1 Schematic illustration of the concept for a flexible and stretchable bionic TRNG, where process flow of the bionic TRNG film manufacture, generating method of the laser speckle, post-processing, randomness tests, and the wearable application are depicted.

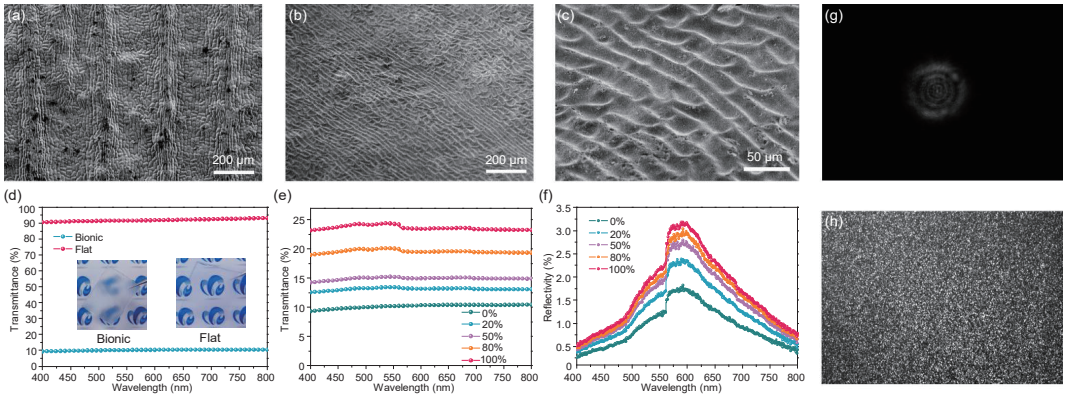

Figure 2 Characterization of template, as-fabricated films, and speckles. (a) Top-view SEM of a ginkgo leaf. (b) 45° tilted-view morphology of the bionic RNG templating from ginkgo leaf. (c) Magnified view of panel (b). (d) Transmittance of the bionic TRNG film and the flat PDMS film, where the insets are the actual photographs of the two films. (e) Transmittance and (f) reflectivity of the bionic TRNG film under different strain. Laser speckle responses of (g) the flat PDMS film and (h) the bionic TRNG.

After performing the soft lithography process, abionic PDMS film molded from the ginkgo leaf is obtained. As shown in the 45° tilted SEM image of Fig. 2(b), the negative structures of the template are successfully molded, which look like continuous random distributed gully-shaped grooves. From the enlarged-view SEM image shown in Fig. 2(c), we can see that the stochastic microgrooves possess different sizes, whose interval distances range from 7 to 43 μm with an average of 22.8 μm (see Fig. S3 in the ESM). Figure 2(d) shows the optical transmittance spectra of the bionic TRNG film, where the transmittance of flat PDMS film without any microstructure is also comparatively investigated. In addition, two actual photos in insets of Fig. 2(d) show a haze bionic TRNG film and a transparent flat film, respectively. At the aforementioned laser wavelength of 638 nm, the flat PDMS film shows high transmittance of about 92%, whereas the transmittance of the bionic film is just 10.4%. The comparison indicates that the microstructures on the surface of the bionic film play key roles in the haze phenomenon. To further study its optical properties under stretched state, we tested the haze, transmittance, and reflectivity of the flexible bionic film in different strain (20%, 50%, 80%, and 100%). With increasing strain, the haze of the bionic film is decreased from 89.6% at 0% strain to 85.11% at 100% strain (see Fig. S4 in the ESM). On the contrary, the transmittance increases with increasing strain, achieving a transmittance of 23.5% at 100% strain and wavelength of 638 nm as shown in Fig. 2(e). Accompanied by the same trend, the reflectivity at 638 nm increases from 1.38 % at non-stretched state to 2.48% at 100% strain (Fig. 2(f)), which demonstrates the light absorptivity of this film decreases with increasing strain. Figure 2(g) shows the laser speckle pattern of flat PDMS film tested by the optical platform introduced in Fig. S1 in the ESM. Only a small multi-layer circular intensity pattern is detected in the center of the image, which is similar to the laser intensity pattern tested without any intermediate solid medium (see Fig. S5 in the ESM). When replaced with the bionic film, scattering occurs between the input laser and the surface microstructures of the bionic film. Consequently, a speckle pattern randomly spreading the whole image is obtained as shown in Fig. 2(h), which indicates the indispensable role of the bionic microstructures on the TRNG. In view of this, we also predict that not only the architectures of ginkgo leaves studied here, but many other natural plants might be used in the mould printing of flexible TRNG films.

In our scheme, the origin of randomness is determined by the physical process of highly complex coherent multiple-scattering [8], where stochastic bionic structures provide an essential basis for this phenomenon. On the one hand, the surface microstructures of bionic film are naturally stochastic, specifically as the different size and diverse distribution direction of each microgrooves. On the other hand, coherent multiple-scattering between incident light and stochastic microstructures plays a pivotal role for random number generation, which exhibits a high degree of complexity and unpredictability. During the experiment, coherent light is modulated by loading different phase patterns into SLM and converted to different high-dimensional spatial light, leading to a large amount of unpredictable coherent multiple-scattering. These different coherent multiple-scattering can be simply recorded in form of speckle patterns, which can be processed into unique random sequences. Meanwhile, it is worth stressing that even only a small variation of coherent light would lead to an absolutely different random sequence [8, 45].

2.2 Speckle analysis

To confirm the physical foundation of the bionic TRNG, a pre-analysis of raw speckle patterns was performed in terms of Euclidean distance and Hamming distance, which are two common metrics to compare the differences between two bit-strings with same length. Specifically, Euclidean distance measures the geometric distance by taking the two strings as vectors in Euclidean space [46], while Hamming distance counts the number of positions towards bit-by-bit dissimilarities [8]. Under the same SLM configuration, 200 speckle images are recorded to estimate the noise of the system. Another 200 speckle images under the different SLM configurations are collected to assess the unpredictability of the system. The histograms of Euclidean distances between normalized images and Hamming distances between images processed by Gabor hash algorithm [8] are visualized in Figs. 3(a) and 3(b), respectively. As seen in Euclidean distances metrics (Fig. 3(a)), the mean value of noise distribution (28.00 ± 4.68) is relatively low compared to unpredictability distribution (572.46 ± 13.61) and there is no overlap between the two distributions, indicating high stability of the system. In Hamming distance metrics (Fig. 3(b)), the unpredictability distribution has a mean value of 0.4964 with a standard deviation of 0.0037. Correspondingly, the coefficient of variation (ratio of standard deviation to mean) is calculated to be 0.0075 approaching to zero, implying a well-concentrated unpredictability distribution. Overall, the well-concentrated distribution and the mean value exceedingly closing to 0.5 reveal a high degree of unpredictability of system under the different SLM configurations, providing the imperative prerequisite for random number generation of the flexible TRNG.

During the process of random number generation, evaluating the amount of speckle randomness is highly significant for

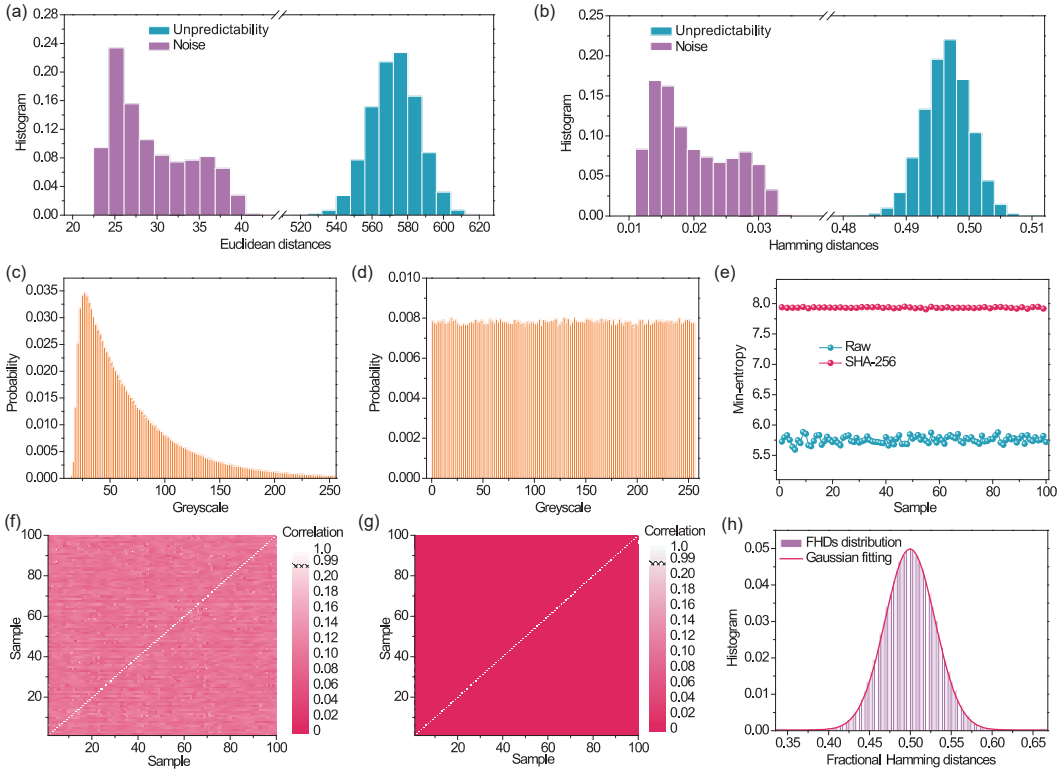

Figure 3 Process of randomness evaluation and extraction. (a) Histograms of Euclidean distances for noise and unpredictability. (b) Histograms of Hamming distances for noise and unpredictability. (c) Probability distribution of greyscale for a raw speckle image. (d) Probability distribution of greyscale for the hashed speckle image. (e) The min-entropy of speckle images before and after randomness extraction. (f) The Pearson correlation coefficient between 100 different raw speckle images. (g) The Pearson correlation coefficient between hashed speckle images. (h) Hamming distance distribution over 256-bit long strings.

subsequent randomness extraction. The randomness of raw speckle images under different SLM configurations has been assessed by means of the min-entropy, which served as the conservative measure of randomness [47, 48]. In our scenario, the min-entropy (E) of an 8-bit greyscale speckle image can be defined as follows

$$E = -\log_2\left(\max_{i\in(0,255)^n} P_i\right) \quad (1)$$

where P_i represents the probability of gray level i in a speckle image. From this, the average min-entropy of raw images is calculated to be 5.756, meaning that only 5.756 information-theoretically random bits can be obtained from the raw 8-bit, which is far from the ideal min-entropy of 8. Meanwhile, the greyscale probability distribution of all pixels for the raw image shows a nonuniformity feature (Fig. 3(c)). The actual min-entropy and the nonuniform greyscale distribution indicate an imperfect randomness, and it is imperative to carry out randomness extraction of raw speckle images. In this work, Secure Hash Algorithm SHA-256 is applied to extract the randomness of speckle images, which cannot be attacked until now [49]. According to the min-entropy analysis, the optimal extraction ratio is calculated to be 5.756/8 ≈ 0.72 under the premise of generating random bits with high-quality randomness. Correspondingly, the input bit-string length should be at least 256 × 8/5.756 ≈ 356 bits due to the fact that SHA-256 hash function has a fixed output length of 256 bits. Given the above analysis, we adopt 100 raw speckle images to produce random binary sequence with the optimal extraction ratio of 0.72. Importantly, greyscale information present in the raw speckle images has been fully mined, where the utilized greyscale information in every pixel is converted to 8-bit binary number. Subsequently, a large amount of binary numbers is processed with SHA-256 hash function to generate 256-bit long strings and these long strings are concatenated into random binary sequence. Compared with the raw image, the greyscale probability distribution of the hashed image displays a uniformly statistical characteristics (Fig. 3(d)), indicating the effectiveness for randomness extraction. We also count the frequency of 0/1 bit in the hashed images, which is exhibited in Fig. S6 in the ESM. The bit 0/1 percentage in every image is almost same, revealing all the hashed images with good uniformity. In addition, the min-entropy of hashed images nearly approaches the ideal value of 8 as shown in Fig. 3(e), which reveals a perfect randomness of hashed images after randomness extraction.

The correlation between speckle images is an essential indicator for random number generation. Typically, Pearson correlation coefficient is commonly used to characterize the relationship between images [50], which is defined by the following equation

$$R = \frac{\sum_{i=1}^{N}(X_i - \mu_X)(Y_i - \mu_Y)}{(N-1)\sigma_X\sigma_Y} \quad (2)$$

where X_i and Y_i is the greyscale value of the i^{th} pixel in image X and Y, μ_X and μ_Y is the mean greyscale value in image X and Y, σ_X and σ_Y is the standard deviation of greyscale value in image X and Y, and N is the total number of pixels. Figure 3(f) shows the correlation coefficient between 100 different raw images and the correlation coefficient is of the order of 10^{-1}. In comparison, as depicted in Fig. 3(g), correlation coefficient between hashed images declines to the order of 10^{-4}, which is sufficiently small to illustrate the almost ideal unpredictability and independence between hashed results [28]. The correlation coefficient before and after randomness extraction also clearly depicts the same regularity (see Fig. S7 in the ESM). That is, ultra-low correlation, desirable unpredictability, and independence represent a satisfying feature of generated random sequence.

To further elucidate the randomness nature of the flexible TRNG, we consider Hamming distance distribution among a large quantity of 256-bit long strings composing random binary

sequence. The Hamming distance distribution is obtained from 5, 000 256-bit long strings compared with each other as visualized in Fig. 3(h). Remarkably, the Hamming distance reveals a near-perfect Gaussian distribution with a mean value of 0.50001 and a standard deviation of 0.03125. The degrees-of-freedom (F) of long strings can be evaluated using the following equation [8]

$$F = \frac{\mu \times (1-\mu)}{\sigma^2} \approx 256 \quad (3)$$

where μ is the mean value, and σ is the standard deviation. It is obvious that these long strings manifest the high degrees-of-freedom of up to 256, which are equivalent to the length of long strings, implying that long strings with full entropy are obtained and each bit presents its independent randomness. Accordingly, we have sufficiently extracted the randomness from raw speckle images. For clarity, the whole process of randomness extraction is summarized in the flow chart (Fig. S8 in the ESM).

2.3 Randomness evaluation

Here, a thorough randomness analysis of the proposed bionic RNG is conducted by running well-known randomness battery of tests including NIST SP800-22 [51], TestU01 Alphabit [52], and DIEHARDER [53]. To this end, we have generated a large file of 1 Gbit random bit streams from 38 successive raw speckle images, and the random bit streams are provided as inputs to these statistical testing suites.

The NIST statistical test suite, served as an initial evaluation for cryptographic applications, is comprised of 15 different statistical tests and each test produces several p-values. The bit length of each tested sequence is required to be within the interval 10^3–10^7 according to test protocol. In our case, the random bit streams are read and divided up into 1,000 blocks of 1 Mbit for the NIST suite, which return the results of two important indicators, uniformity of p-values and pass rate (proportion of sequences passing a test). As proposed by NIST, alpha significance level of 0.01 has been identified. The NIST results of 15 statistical tests are displayed in Fig. 4(a), where all the p-values are in a range from 0.01 to 0.99. Intuitively, uniformity of p-values is all greater than 10^{-4} and passed proportions lie above the required minimum (98%) (detailed values can be seen in Table S1 of the ESM). Due to this fact, the 1 Gbit random bit streams is considered to successfully pass the NIST suite.

The next suite TestU01 is a widely adopted library for randomness test, which has been developed by Pierre L'Ecuyer and Richard Simard for empirical statistical tests of random numbers. With the goal of evaluating physical TRNGs, we apply Alphabit battery with a collection of 17 statistical tests to estimate the randomness of the bionic TRNG. According to TestU01 test standards, the 1 Gbit random bits streams from bionic TRNGs is converted into a binary file to fulfill the requirement. In order to pass the Alphabit battery, all the p-values of 17 different statistical tests should fall into the range of [0.001, 0.999]. Figure 4(b) and Table S2 in the ESM show the results of TestU01 Alphabit buttery. From all this, the binary random sequence passes all the statistical tests.

We also apply more stringent and demanding statistical test suite for our generated random bit streams, the so-called DIEHARDER tests [53]. In 1995, George Marsaglia designed DIEHARD battery of test and it has been widely applied in random number test suites. Later Robert G. Brown modified and expanded DIEHARD into the DIEHARDER test suite, which incorporates 17 tests from DIEHARD battery and 14 extended test items. The DIEHARDER battery of test is performed with default settings and visualized results are shown in Fig. 4(c) (detailed results can be found in Table S3 in the ESM). In terms of evaluation criterion, a test item is labeled as "PASSED" only when its corresponding p-value is within the interval [0.005, 0.95]. In our results, it manifests that none of p-values skip the interval.

In a nutshell, we have performed an in-depth analysis of the proposed TRNG and the random bit streams pass all the randomness battery of tests successfully, indicating a high-quality and efficient bionic RNG for random number generation. In our particular case, almost 27.54 Mbit random bits are extracted from a raw speckle image under the extraction ratio of 72%. Therefore,

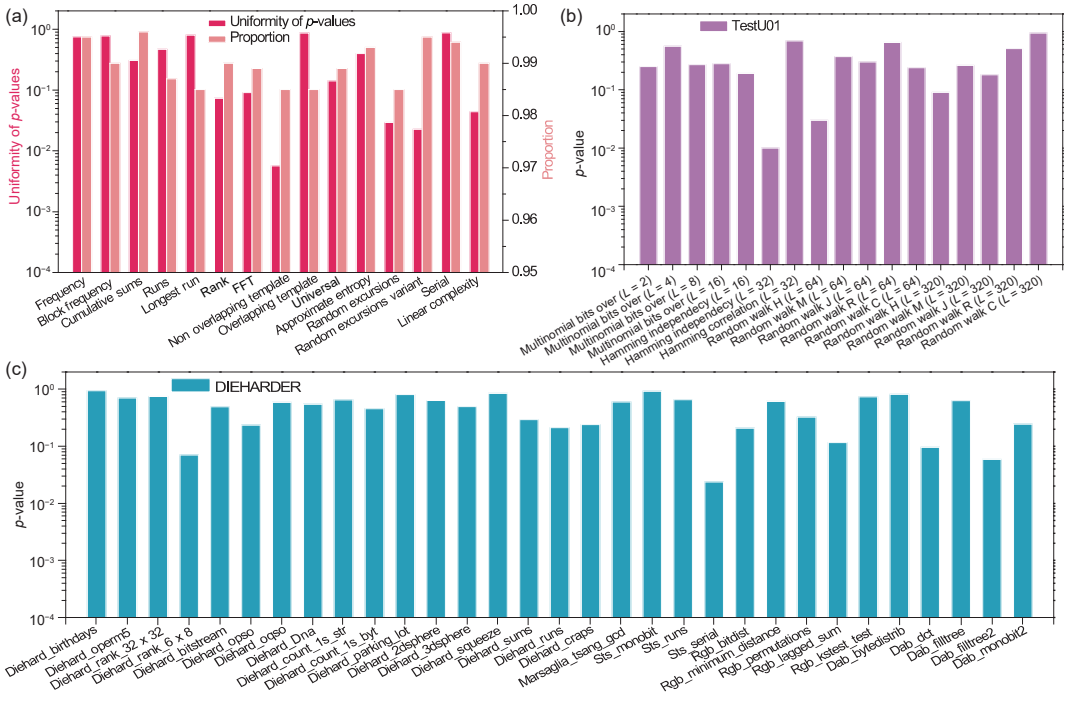

Figure 4 Randomness battery of tests. (a) NIST results for uniformity of p-values and passed proportions of 15 statistical tests. A uniformity of p-values > 10^{-4} and a proportion > 0.98 are required for each test item to pass. (b) TestU01 Alphabit results for the p-values of the 17 statistical tests. When the p-value is larger than 0.001 and smaller than 0.999, the test is regard as a success. (c) DIEHARDER results for 31 test items.

there is a random number generation rate of approximately 1.04 Gbit/s with a typical camera frame rate of 39 fps. In the foreseeable future, the random number generation rate of the flexible TRNG can be elevated to several hundreds of Gbit/s if we implement a high-speed digital micromirror device and a comparable camera in our scheme.

2.4 Mechanical robustness tests

Stretchability is a key element of mechanical adaptability for flexible electronics [43]. Figure 5(a) shows the flexible TRNG film with different strains of 0%, 50%, and 150%. No fracture is found until strain exceeds 200%. Meanwhile, we study the properties of output speckle with increasing strain upon a fixed modulated input laser. As a result, Hamming distances between the speckle patterns of the TRNG film being stretched and the initial speckle, grow with increasing strain, rising to a saturation value of about 0.5 at 3% strain as shown in Fig. 5(b). We can see that the output speckle images are very sensitive to applied slight strains. In other words, when strain exceeds 3%, the output speckle patterns have been totally different with initial speckle image. Actually, these variations cannot affect random number generation even if the flexible TRNG film is deformed under mechanical force. In addition, correlation coefficients between 10 speckle patterns under different strains from 0% to 100% were also investigated as displayed in Fig. 5(c). All of the correlation coefficients are below 0.05, once again confirming that the stretching strain is beneficial for the flexible TRNG to generate more random numbers.

To evaluate the mechanical robustness, we investigated the min-entropy of the flexible TRNG suffered from mechanic shocks including cyclic stretching, cyclic bending and temperature shock. During cyclic stretching with 50% strain and cyclic bending with bending radius of 5 mm, we assess the min-entropy of output speckle patterns every thousand cycles. The dot and line chart of obtained min-entropy along with stretching cycles in Fig. 5(d) shows that all the min-entropy is always consistent with the initial state, which demonstrates a considerable information volume of output speckle patterns. Similarly, the min-entropy also shows a superior stability compatible with the original condition after 10, 000 times cyclic bending as shown in Fig. 5(e). From the SEM image of the bionic film after 10,000 times stretching or bending (see Fig. S9 in the ESM), no micro-fractures and damages are found, and the surface still remains the basic morphology with Fig. 2(b), showing the robustness of the flexible TRNG film itself. To estimate the performance of the flexible TRNG against temperature shock, we study the laser speckle responses of the film under different temperature conditions ranging from −25 to 80 °C. Ultimately, the obtained min-entropy of speckles at different temperatures also shows a stable output as shown in Fig. 5(f) like the results of aforementioned cyclic stretching or bending tests, which reveals the thermal reliability of the TRNG within a certain temperature range. Moreover, the TRNG can also continue to work stably when exposed to low (−25 °C) or high (80 °C) temperatures for at least 24 hours (see Fig. S10 in the ESM). In comparison to other generating methods of true random numbers (Table 1), the bionic TRNG in this work shows obvious advantages over many other options in all of aspects including higher generation rate, more typical randomness test suites, and excellent mechanical robustness such as flexibility, stretchability, and resistance to temperature shock.

2.5 Wearable applications

Emerging portable and wearable networked electronics further require low-cost, mechanically flexible, and body-compatible security hardware components. Here, we fabricated a wearable wristband by using the flexible TRNG film as shown in Fig. 6(a). Unlike aforesaid implementation of transmitted laser speckle, the reflected laser speckle has been also investigated in this scenario. As illustrated in Fig. S11 in the ESM, modulated laser beam with a specific angle was objected onto the microstructured surface of the TRNG film. Then, the reflected speckle was collected by the CCD camera. After post-processing, a series of credible random numbers is obtained as shown in Fig. 6(b). Significantly, the wearable wristband could work under water (Fig. 6(c)) and successfully generate true random numbers (Fig. 6(d)). In addition, the flexible TRNG film attached to a curved entity underwater could also stably output random numbers (see Figs. 6(e) and 6(f)), which indicates a promising potential that can be integrated with specific flexible electronic systems and applied in underwater environment. Given the advantageous performance of the flexible TRNG, we propose a concept of encrypted communication between networked components of deep-sea exploration system based on the flexible TRNG. Typically, some sensitive tasks like special army operations or secret resource exploration in the deep sea require random numbers for encryption and communication.

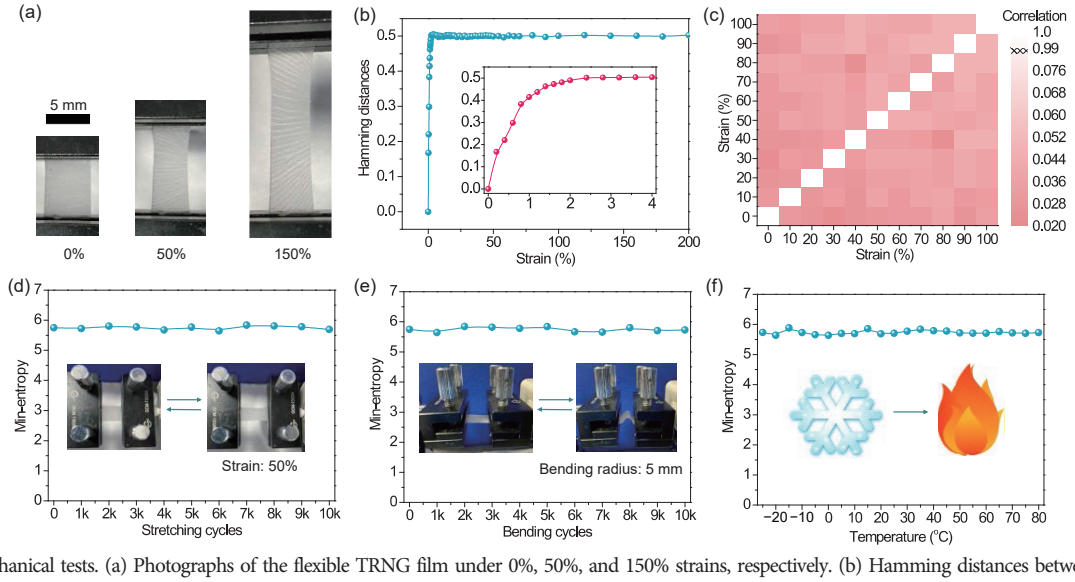

Figure 5 Mechanical tests. (a) Photographs of the flexible TRNG film under 0%, 50%, and 150% strains, respectively. (b) Hamming distances between the speckle patterns under different strains upon a constant laser input and the original speckle, where the inset is the enlarged data within 4% strain. (c) Color mapping of correlation coefficient between 10 speckle patterns under different strains. (d) Min-entropy of the flexible TRNG during cyclic stretching of 50% strain. (e) Min-entropy of the flexible TRNG during cyclic bending with bending radius of 5 mm. (f) Min-entropy of the flexible TRNG against different temperatures from −25 to 80 °C.

Table 1 Comparisons with other TRNGs

TRNG	Entropy source	Generation speed	Mechanics	Verification
Yu 2016 [26]	RTN of triboelectric generator	Not available	Rigid	Mainly tested uniformity and autocorrelation
Rojas 2017 [23]	RTN of transistor	Not available	Unstretchable	Passed NIST with 9 items and TestU01
Jiang 2017 [18]	RTN of memristor	6 kbit/s	Rigid	Passed NIST
Meiser 2020 [38]	Random DNA syntheses	2.4 Mbit/s	Rigid	Passed NIST with 9 items
Lee 2020 [37]	Random crystallization images	200 kbit/s	Rigid	Passed NIST
Kim 2020 [27]	RTN of triboelectric generator	20 kbit/s	Rigid	Passed NIST
Brown 2020 [24]	RTN of transistor	19.2 kbit/s	Rigid	Passed NIST and DIEHARD
Wen 2021 [21]	RTN of memristor	1 Mbit/s	Rigid	Passed NIST
Li 2021 [22]	RTN of memristor	1 Mbit/s	Rigid	Passed NIST
This work	Random laser speckles of the bionic TRNG	1.04 Gbit/s	Flexible, stretchable, and thermally stable	Passed all items of NIST, TestU01, and DIEHARDER

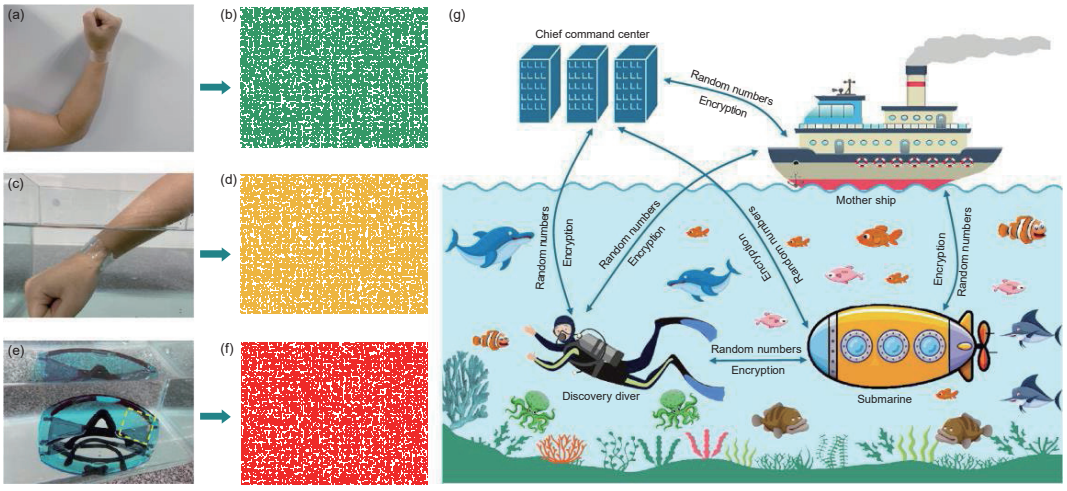

Figure 6 Application demonstrations. (a) Photo image of the flexible TRNG as a wearable wristband and (b) its output random numbers (white "1" green "0"). (c) Image of the wearable TRNG wristband underwater and (d) its generated random numbers (white "1", yellow "0"). (e) Photograph of the TRNG as a flexible label attached to a curved entity underwater and (f) its produced random numbers (white "1", red "0"). (g) A schematic concept of the application of the flexible TRNG in encrypted communication between networked components of the deep-sea exploration system.

As demonstrated in Fig. 6(g), submarine carrying discovery diver dives into the deep sea from the mother ship. After reaching the target sea area, the discovery diver leaves away submarine and executes secret missions. In this system, flexible TRNGs are integrated with wearable device of discovery diver and flexible platforms of submarine, mother ship, and chief command center. All of the components in the system are networked together by using random numbers to communicate sensitive encrypted information such as instruction, findings, and their respective positions.

3 Conclusions

In summary, inspired by the natural unique and random biological architectures, we propose a flexible and stretchable bionic TRNG by molding the surface microstructures of a ginkgo leaf. The manufacturing process is simple, low-cost, green, and environmentally friendly. The flexible TRNG exhibits a fast generation speed of 1.04 Gbit/s with a high extraction rate of 72% and superior flexibility that can be stretched to 200% strain. Remarkably, extracted random numbers possess expected randomness, and successfully pass all randomness test suites including NIST, TestU01, and DIEHARDER. In addition, the TRNG also shows robust mechanical reliability under bellowing conditions: (i) 10,000 times cyclic stretching with 50% strain; (ii) 10,000 times cyclic bending (bending radius, 5 mm) tests; (iii) wide-range temperature shock (−25–80 °C). More significantly, the bionic TRNG could be operated as a wearable wristband or a flexible label attached to a curved entity under diversified scenarios. Based on the above advantageous performances of the flexible TRNG, a concept of encrypted communication between networked components of a deep-sea exploration system is proposed. We expect that the flexible and stretchable bionic TRNG could provide a promising potential for safeguarding the information security of emerging flexible networked electronics.

4 Experimental section

4.1 Fabrication of the bionic TRNG film

First, the ginkgo leaf was cut into rectangular shapes and washed with deionized water three times. After being dried via N_2 gas blowing, the ginkgo leaf template was fixed on aglass substrate using Scotch tape. Then, PDMS (Sylgard 184, Dow Corning) mixture liquid with a base-to-curing agent ratio of 10:1 was evenly coated onto the surface of the ginkgo leaf template. After curing at 70 °C for 1 hour, the PDMS film with the inverse structure of the biological architectures was finally peeled off as the bionic TRNG film.

4.2 Characterization setups

The surface morphology of the ginkgo leaf and bionic TRNG film was investigated using a scanning electron microscope (SEM, Carl Zeiss SUPRA60) operated at 2.5 kV. The haze of the TRNG film

was tested by a high-precision spectral haze meter (EVERFINE Corporation, HAM300). The transmittance and reflectivity of the bionic film were examined using a ultraviolet–visible–infrared (UV–Vis–IR) spectrophotometer (Wavetest, Lambda950). For the bending or stretching tests, the TRNG film was clamped on a home-made flexibility tester and subjected to different strain or bending radii. The laser speckles were investigated intensively in our optical system platform (see schematic illustration of Fig. S1 in the ESM) as depicted in the following steps. (i) A collimated and expanded compact laser beam with central wavelength of 638 nm (Integrated Optics, No. 0638L-11A) goes through the beam splitter and illuminates aphase-only liquid crystal SLM (1,920 × 1, 080 pixels, pixel size = 8.0 μm, Holoeye, PLUTO-2-VIS-014), on which pseudo random patterns are used as challenges by modulating the laser beam wavefront through randomly setting each pixel's value. (ii) After penetrating through the lens and the iris, the input challenge projects onto the front surface of the bionic TRNG film. (iii) Hereafter, the transmitted or reflected speckle patterns are collected using a CCD camera with a frame rate of 39 fps at 2,448 × 2,048 pixels (FLIR, GS3-U3-51S5M). (iv) Consequently, the speckle patterns were filtered into random bit streams via our in-house-developed post-processing algorithm, and the randomness performances of the flexible TRNG are evaluated using randomness test suites including NIST, TestU01, and DIEHARDER. More details about the whole process of randomness extraction can be seen in Fig. S8 in the ESM.

Acknowledgements

This study was financially supported by the funds of the Science Challenging Project (No. TZ2018003) and the National Natural Science Foundation of China (Nos. 12175204, 61875178, 61805218, and 12104423).

Author contributions

Y. Wan and K. Chen contributed equally to this work. Y. Wan and Y. Yao conceived the idea. Y. Yao supervised the project. Y. Wan, K. Chen, and Z. Qiu implemented the main experiments.F. Huang, P. Wang, X.Leng, D. Li, and J. Kang participated in experiment discussions. Y. Wan and Z. Qiu designed the schematic diagrams. Y. Wan, K. Chen, and Y. Yao drafted the manuscript. All authors contributed to the revised manuscript.

Electronic Supplementary Material: Supplementary material (light path diagram of transmitted laser speckle, pseudo random pattern, statistical distribution of bionic microstructures, haze of the bionic TRNG film, multi-layer circular laser intensity pattern, percentage of bit 0/1 for different hashed images, Pearson correlation coefficient between 100 different speckle images, the whole process of randomness extraction, SEM images of the flexible TRNG film after 10,000 times stretching and bending, continuous work stability of the TRNG at low or high temperature, light path diagram of reflective laser speckle, and detailed randomness test results of NIST, TestU01, and DIEHARDER) is available in the online version of this article at https://doi.org/10.1007/s12274-022-4109-9.

References

[1] Marx, V. The big challenges of big data. *Nature* **2013**, *498*, 255–260.
[2] Yang, Y. Multi-tier computing networks for intelligent IoT. *Nat. Electron.* **2019**, *2*, 4–5.
[3] Sfar, A. R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the internet of things. *Digital Commun. Netw.* **2018**, *4*, 118–137.
[4] Wan, Y. B.; Wang, P. D.; Huang, F.; Yuan, J.; Li, D.; Chen, K.; Kang, J. B.; Li, Q.; Zhang, T. P.; Sun, S. et al. Bionic optical physical unclonable functions for authentication and encryption. *J. Mater. Chem. C* **2021**, *9*, 13200–13208.
[5] Jin, C.; Chen, W. X.; Cao, Y. K.; Xu, Z. W.; Tan, Z. M.; Zhang, X.; Deng, L.; Zheng, C. S.; Zhou, J.; Shi, H. S. et al. Development and evaluation of an artificial intelligence system for COVID-19 diagnosis. *Nat. Commun.* **2020**, *11*, 5088.
[6] Karaklajić, D.; Schmidt, J. M.; Verbauwhede, I. Hardware designer's guide to fault attacks. *IEEE Trans. Very Large Scale Integr. Syst.* **2013**, *21*, 2295–2306.
[7] Mao, S. F.; Wolf, T. Hardware support for secure processing in embedded systems. *IEEE Trans. Comput.* **2010**, *59*, 847–854.
[8] Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030.
[9] Fischer, I.; Gauthier, D. J. High-speed harvesting of random numbers. *Science* **2021**, *371*, 889–890.
[10] Wang, P. D.; Chen, F. L.; Li, D.; Sun, S.; Huang, F.; Zhang, T. P.; Li, Q.; Chen, K.; Wan, Y. B.; Leng, X. et al. Authentication of optical physical unclonable functions based on single-pixel detection. *Phys. Rev. Appl.* **2021**, *16*, 054025.
[11] Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715.
[12] Chen, S. Random number generators go public. *Science* **2018**, *360*, 1383–1384.
[13] Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
[14] Barreno, M.; Nelson, B.; Joseph, A. D.; Tygar, J. D. The security of machine learning. *Mach. Learn.* **2010**, *81*, 121–148.
[15] Varnava, C. FinFETs for cryptography. *Nat. Electron.* **2020**, *3*, 732–732.
[16] Skrzypczyk, P. Predictably random. *Nat. Phys.* **2021**, *17*, 431–432.
[17] Chen, K.; Huang, F.; Wang, P. D.; Wan, Y. B.; Li, D.; Yao, Y. Fast random number generator based on optical physical unclonable functions. *Opt. Lett.* **2021**, *46*, 4875–4878.
[18] Jiang, H.; Belkin, D.; Savel'ev, S. E.; Lin, S. Y.; Wang, Z. R.; Li, Y. N.; Joshi, S.; Midya, R.; Li, C.; Rao, M. Y. et al. A novel true random number generator based on a stochastic diffusive memristor. *Nat. Commun.* **2017**, *8*, 882.
[19] Woo, K. S.; Wang, Y. M.; Kim, Y.; Kim, J.; Kim, W.; Hwang, C. S. A combination of a volatile-memristor-based true random-number generator and a nonlinear-feedback shift register for high-speed encryption. *Adv. Electron. Mater.* **2020**, *6*, 1901117.
[20] Kim, G.; In, J. H.; Kim, Y. S.; Rhee, H.; Park, W.; Song, H. C.; Park, J.; Kim, K. M. Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor. *Nat. Commun.* **2021**, *12*, 2906.
[21] Wen, C.; Li, X. H.; Zanotti, T.; Puglisi, F. M.; Shi, Y. Y.; Saiz, F.; Antidormi, A.; Roche, S.; Zheng, W. W.; Liang, X. H. et al. Advanced data encryption using 2D materials. *Adv. Mater.* **2021**, *33*, 2100185.
[22] Li, X. H.; Zanotti, T.; Wang, T.; Zhu, K. C.; Puglisi, F. M.; Lanza, M. Random telegraph noise in metal-oxide memristors for true Random number generators: A materials study. *Adv. Funct. Mater.* **2021**, *31*, 2102172.
[23] Gaviria Rojas, W. A.; McMorrow, J. J.; Geier, M. L.; Tang, Q. Y.; Kim, C. H.; Marks, T. J.; Hersam, M. C. Solution-processed carbon nanotube true random number generator. *Nano Lett.* **2017**, *17*, 4976–4981.
[24] Brown, J.; Zhang, J. F.; Zhou, B.; Mehedi, M.; Freitas, P.; Marsland, J.; Ji, Z. G. Random-telegraph-noise-enabled true random number generator for hardware security. *Sci. Rep.* **2020**, *10*, 17210.
[25] Wali, A.; Ravichandran, H.; Das, S. A machine learning attack resilient true Random number generator based on stochastic programming of atomically thin transistors. *ACS Nano* **2021**, *15*, 17804–17812.
[26] Yu, A. F.; Chen, X. Y.; Cui, H. T.; Chen, L. B.; Luo, J. J.; Tang, W.; Peng, M. Z.; Zhang, Y.; Zhai, J. Y.; Wang, Z. L. Self-powered random number generator based on coupled triboelectric and electrostatic induction effects at the liquid–dielectric interface. *ACS Nano* **2016**, *10*, 11434–11441.
[27] Kim, M. S.; Tcho, I. W.; Park, S. J.; Choi, Y. K. Random number generator with a chaotic wind-driven triboelectric energy harvester.

Nano Energy **2020**, *78*, 105275.
[28] Kim, K.; Bittner, S.; Zeng, Y. Q.; Guazzotti, S.; Hess, O.; Wang, Q. J.; Cao, H. Massively parallel ultrafast random bit generation with a chip-scale laser. *Science* **2021**, *371*, 948–952.
[29] Uchida, A.; Amano, K.; Inoue, M.; Hirano, K.; Naito, S.; Someya, H.; Oowada, I.; Kurashige, T.; Shiki, M.; Yoshimori, S. et al. Fast physical random bit generation with chaotic semiconductor lasers. *Nat. Photonics* **2008**, *2*, 728–732.
[30] Kanter, I.; Aviad, Y.; Reidler, I.; Cohen, E.; Rosenbluh, M. An optical ultrafast random bit generator. *Nat. Photonics* **2010**, *4*, 58–61.
[31] Bai, B.; Huang, J. Y.; Qiao, G. R.; Nie, Y. Q.; Tang, W. J.; Chu, T.; Zhang, J.; Pan, J. W. 18.8. Gbps real-time quantum random number generator with a photonic integrated chip. *Appl. Phys. Lett.* **2021**, *118*, 264001.
[32] Gabriel, C.; Wittmann, C.; Sych, D.; Dong, R. F.; Mauerer, W.; Andersen, U. L.; Marquardt, C.; Leuchs, G. A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* **2010**, *4*, 711–715.
[33] Avesani, M.; Marangon, D. G.; Vallone, G.; Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. *Nat. Commun.* **2018**, *9*, 5365.
[34] Liu, Y.; Zhao, Q.; Li, M. H.; Guan, J. Y.; Zhang, Y. B.; Bai, B.; Zhang, W. J.; Liu, W. Z.; Wu, C.; Yuan, X. et al. Device-independent quantum random-number generation. *Nature* **2018**, *562*, 548–551.
[35] Luo, Q.; Cheng, Z. D.; Fan, J. K.; Tan, L. J.; Song, H. Z.; Deng, G. W.; Wang, Y.; Zhou, Q. Quantum random number generator based on single-photon emitter in gallium nitride. *Opt. Lett.* **2020**, *45*, 4224–4227.
[36] Sznitko, L.; Chtouki, T.; Sahraoui, B.; Mysliwiec, J. Bichromatic laser dye as a photonic Random number generator. *ACS Photonics* **2021**, *8*, 1630–1638.
[37] Lee, E. C.; Parrilla-Gutierrez, J. M.; Henson, A.; Brechin, E. K.; Cronin, L. A crystallization robot for generating true random numbers based on stochastic chemical processes. *Matter* **2020**, *2*, 649–657.
[38] Meiser, L. C.; Koch, J.; Antkowiak, P. L.; Stark, W. J.; Heckel, R.; Grass, R. N. DNA synthesis for true random number generation. *Nat. Commun.* **2020**, *11*, 5869.
[39] Pironio, S.; Acín, A.; Massar, S.; de la Giroday, A. B.; Matsukevich, D. N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T. A.; Monroe, C. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024.
[40] Wan, Y. B.; Qiu, Z. G.; Huang, J.; Yang, J. Y.; Wang, Q.; Lu, P.; Yang, J. L.; Zhang, J. M.; Huang, S. Y.; Wu, Z. G. et al. Natural plant materials as dielectric layer for highly sensitive flexible electronic skin. *Small* **2018**, *14*, 1801657.
[41] Qiu, Z. G.; Wan, Y. B.; Zhou, W. H.; Yang, J. Y.; Yang, J. L.; Huang, J.; Zhang, J. M.; Liu, Q. X.; Huang, S. Y.; Bai, N. N. et al. Ionic skin with biomimetic dielectric layer templated from Calathea zebrineleaf. *Adv. Funct. Mater.* **2018**, *28*, 1802343.
[42] Wan, Y. B.; Qiu, Z. G.; Hong, Y.; Wang, Y.; Zhang, J. M.; Liu, Q. X.; Wu, Z. G.; Guo, C. F. A highly sensitive flexible capacitive tactile sensor with sparse and high-aspect-ratio microstructures. *Adv. Electron. Mater.* **2018**, *4*, 1700586.
[43] Wan, Y. B.; Wang, Y.; Guo, C. F. Recent progresses on flexible tactile sensors. *Mater. Today Phys.* **2017**, *1*, 61–73.
[44] Qin, D.; Xia, Y. N.; Whitesides, G. M. Soft lithography for micro- and nanoscale patterning. *Nat. Protoc.* **2010**, *5*, 491–502.
[45] Pappu, R. S. Physical one-way functions. Ph. D. Dissertation, Massachusetts Institute of Technology, Cambridge, MA, USA, 2001.
[46] Zhang, J. *Visualization for Information Retrieval*; Springer Science & Business Media: New York, 2007.
[47] Rényi, A. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability,* Berkeley, USA, 1961, pp 547–561.
[48] Ma, X. F.; Xu, F. H.; Xu, H.; Tan, X. Q.; Qi, B.; Lo, H. K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **2013**, *87*, 062327.
[49] Sadat, M. N.; Aziz, M. M. A.; Mohammed, N.; Pakhomov, S.; Liu, H. F.; Jiang, X. Q. A privacy-preserving distributed filtering framework for NLP artifacts. *BMC Med. Inform. Decis. Mak.* **2019**, *19*, 183.
[50] Ji, L.; Gallo, K. An agreement coefficient for image comparison. *Photogramm. Eng. Rem. Sens.* **2006**, *72*, 823–833.
[51] Rukhin, A.; Soto, J.; Nechvatal, J. R.; Smid, M. E.; Barker, E. B.; Leigh, S. D.; Levenson, M.; Vangel, M., Banks, D. L.; Heckert, N. A. et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800–22, Revision 1a, 2010.
[52] L'Ecuyer, P.; Simard, R. TestU01: A C library for empirical testing of random number generators. *ACM Trans. Math. Software* **2007**, *33*, 22.
[53] Brown, R. G. *Dieharder: A Random Number Test Suite, Version 3.31.1* [Online]. Robert G. Brown, NC, 2022; pp. https://webhome.phy.duke.edu/~rgb/General/dieharder.php (accessed)