scientific reports

Check for updates

OPEN

Cryptographic triboelectric random number generator with gentle breezes of an entropy source

Moon-Seok Kim[1,2,3], Il-Woong Tcho[1,3] & Yang-Kyu Choi[1]✉

A wind-driven triboelectric nanogenerator (W-TENG) is a promising energy harvesting device due to its clean, ubiquitous and unexhausted properties. In addition, a W-TENG induces unpredictable chaotic outputs from wind flow that can serve as an entropy source for cryptography. This can be applied to a true random number generator (TRNG) for a secured system due to its inherent turbulent nature; thus, a W-TENG with a two-in-one structure can simultaneously generate both power and true random numbers. However, a previously reported W-TENG had one major drawback: a wind velocity of 10 m/s is required for stable energy harvesting by wind force. Thus, it is timely to demonstrate a W-TENG-based RNG whose operating condition is below 3 m/s, which is a gentle breeze similar to natural wind. In this study, we demonstrate a wind-driven cryptographic triboelectric random number generator (WCT-RNG) by using a W-TENG whose operating condition for wind speed is below 3 m/s by adopting a rear-fixed film structure instead of a conventional structure. The rear-fixed film refers to the fluttering film being freestanding on the front-side and fixed on the rear-side, where the front- and rear-sides are the wind inlet and outlet, respectively. The WCT-RNG enables the W-TENG to operate below a 3 m/s wind velocity. Because of this, the working time of the WCT-RNG is dramatically enhanced from only 8–42% at an average altitude above sea level. As the capability of operating at low wind speeds is significantly improved, a WCT-RNG becomes more useful and practical for generating both power and true random numbers in a single device. The device can thereby lead to the construction of a self-powered TRNG and secure communication for Internet of Things (IoT) devices in various environments, even under a gentle breeze. In this study, we explain the design of a WCT-RNG structure and also evaluate its randomness by using an NIST SP 800-22 B test suite with a reliability test.

Recently, the Internet of Things (IoT) has emerged as a new computing paradigm that can connect devices, objects, machines, and people through hyper-connectivity[1,2]. Forecasts predict that the number of online IoT devices will exceed 64 billion by 2025, with devices installed in various locations[3]. In IoT and smart system technology, each device commonly provides services to maintain an unexhausted power supply and communicate with other devices[4–6]. To ensure the functioning of IoT systems, it is crucial to install primitives that guarantee security functions for all devices, as IoT security attacks have increased by 77% in 2022 compared to the previous year, totaling 57 million, according to the 2022 Cyber Threat Report by SonicWall[7]. To prevent security threats, each system must have security functions: (i) confidentiality, (ii) integrity, (iii) availability, (iv) authentication, and (v) non-repudiation[8]. A hardware-based security device, known as a true random number generator (TRNG), is essential for supporting the aforementioned security functions as compared to a software-based security primitive, which uses a specific algorithm to generate pseudo-random numbers and is vulnerable to attacks or exploitation[9,10]. Therefore, developing TRNGs for various devices and situations is crucial for achieving secure IoT technology[11,12].

Previously, we demonstrated a TRNG using a prototyped wind-driven triboelectric nanogenerator (W-TENG)[13]. The W-TENG-based TRNG not only provides energy harvesting but also security functions for communication systems such as IoT, smart grids for electricity networks, and in-flight applications. It produces true random numbers by converting chaotic wind flow to a random electrical signal. We demonstrated that the electrical signals directly induced from the W-TENG exhibits randomness without the need of

[1]School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea. [2]The Department of Semiconductor System Engineering, Hanbat National University, 125 Dongseo-daero, Yuseong-gu, Daejeon 31538, Republic of Korea. [3]These authors contributed equally: Moon-Seok Kim and Il-Woong Tcho. ✉email: ykchoi@ee.kaist.ac.kr

post-processing, which is an extra process to manipulate or transform the generated random numbers to meet specific requirements.

However, an operation condition of the abovementioned W-TENG prototype is limited to high wind velocities of over 10 m/s. For practical outdoor use, extending the applicable conditions of the W-TENG to operate in a natural gentle breeze is crucial. In this work, we propose a wind-driven cryptographic triboelectric random number generator (WCT-RNG) that harvests wind energy and generates random numbers under a gentle breeze. The proposed WCT-RNG where the front- and rear-sides are the wind inlet and outlet, respectively adopts the rear-fixed film structure. The WCT-RNG generates electricity with alternating current (AC) at low wind velocities, which is utilized for a random signal source. Unlike a conventional W-TENG with a 4-corner fixed structure that is actuated by strong vortex flow, the WCT-RNG can flutter with laminar flow as well as vortex shedding due to the freestanding nature of the rear-fixed fluttering film even for input wind with a relatively low velocity[14]. This WCT-RNG can help advance secured and self-powered IoT and smart mobile systems through its improved capability to operate using natural wind.

For comparative studies, two types of a conventional W-TENG were used as a control group. Control group I adopted the 4-corner fixed fluttering film structure of conventional W-TENG[13] which is named 4FW-TENG. Control group II employed a decoupled rear-fixed film W-TENG (RFW-TENG) structure. Decoupled RFW-TENGs are systems where the upper and lower TENG units independently generate energy through a separated electrical load. Conversely, a coupled RFW-TENG as an experimental group generates energy through a single common electrical load, which is used for a proposed WCT-RNG.

Materials and methods

Fabrication of WCT-RNG

For this study, we fabricated a WCT-RNG which is fixed at the rear but freestanding at the front; the input wind comes in via the freestanding side and the output wind exits through the fixed side[14]. The freestanding part of the film at the front-side enables the film to flutter with both a laminar and vortex flow; thus, the WCT-RNG can operate at a lower wind velocity compared to conventional W-TENG and FW-TENG. The upper and lower plates were manufactured by 3D printing (3DWOX1 from Sindoh) composed of curable resin. Their sizes are fixed at a length (L) of 72 mm, a width (W) of 34 mm, and a height (H_{PLATE}) of 3 mm with consideration of optimal power density[14].

Aluminum (Al) with a thickness of 0.3 mm was attached to the inner surface of the exoskeleton resin at the upper and lower plates. Then, perfluoroalkoxy (PFA) film with a thickness of 50 μm was attached onto the abovementioned Al plates. Figure S1 describes the structural specifications for the fabricated WCT-RNG.

The fluttering film is composed of quintuple layers, starting from the top layer of nylon, followed by a layer of Al, then a layer of polyimide (PI), followed by another layer of Al, and finally, a layer of nylon at the bottom. Among these layers, the core film at the center is a PI film with a thickness of 50 μm. The design aims to amplify triboelectric effects through physical contact and separation between the PI film and Al electrode[15]. Al with a thickness of 30 nm was deposited onto both sides of the PI film using an evaporator: first on the front side, then on the backside. Afterwards, a nylon coating process was conducted onto the exterior of the Al films. Nylon has excellent homogeneity, mechanical robustness, and thermal stability[16,17]. Thus, nylon serves as a protection layer which can enforce mechanical robustness to the abrasion of the inner Al layer during iterative contact-separation for both the upper and lower plates and the fluttering film. Thus, the proposed WCT-RNG possesses excellent long-term endurance characteristics. The coating process of the nylon is as follows. First, Nylon 6 (Sigma-Aldrich) is dissolved by a solvent (chloroform: 2,2,2-trifluoroethanol = 1:1, v/v). Next, this Nylon 6 solution is spin-coated onto both sides of the Al film at 3000 rpm for 30 s. Finally, the fabricated fluttering film is baked at 150 °C for 10 min in an oven.

The fluttering film is installed between the upper plate and lower plate. The manufactured WCT-RNG has four wedge-structure protrusions, with two wedges on the top plate and two on the bottom plate, as well as two alignment pins on the front-side, as shown in Fig. 2a,b. The fluttering film was punctured to create two holes, with each pin passing through a hole. These two pins act as a stopper to prevent the fluttering film from getting caught inwardly by aligning it inside the punctured holes. Additionally, the WCT-RNG has four supports on the rear-side, with two on the top plate and two on the bottom plate, as shown in Fig. 2a,b. At each supporter, there are two magnets under the upper resin supporter and two magnets over the lower resin supporter. These supporters firmly fix the fluttering film at the rear-side. Note that the total height (H_{TOTAL}) of the WCT-RNG is 18 mm, which is the sum of the height of the upper supporter ($H_{\mathrm{UP\_SUP}} = 7.5$ mm), the two upper magnets ($H_{\mathrm{UP\_MAG}} = 1.0$ mm), the thickness of the fluttering film with the quintuple layers ($H_{\mathrm{FLUTTER}} = 1.0$ mm), the two lower magnets ($H_{\mathrm{LO\_MAG}} = 1.0$ mm), and the lower supporter ($H_{\mathrm{LO\_SUP}} = 7.5$ mm). Figure S1 describes the heights for the fabricated WCT-RNG. For quick optimization of the H_{TOTAL}, two resin supporters were replaced by stacked magnets, as shown in Fig. 4 and Fig. S3. Thus, the H_{TOTAL} is controlled by changing the number of the stacked magnets.

These installed protrusions play a key role in making the fluttering film perform flip-flop actuation at a low wind velocity by facilitating the easy separation from the upper and lower plate, and the alignment pins prevent the fluttering film from curling inward toward the gap at a high wind velocity. Due to these unique structures, the WCT-RNG can work in a gentle breeze to a strong windstorm. In conclusion, the WCT-RNG can operate at a wind velocity of 3 m/s, at which no vortex shedding arises. Relevant dimensions of the WCT-RNG were optimized with reference to a wind velocity of 4 m/s. Moreover, the WCT-RNG can operate stably for more than 96 h at a high wind velocity of 30 m/s, which is comparable to the nominal wind velocity of a hurricane that can cause a human to be taken off their feet or make roof materials begin to come off.

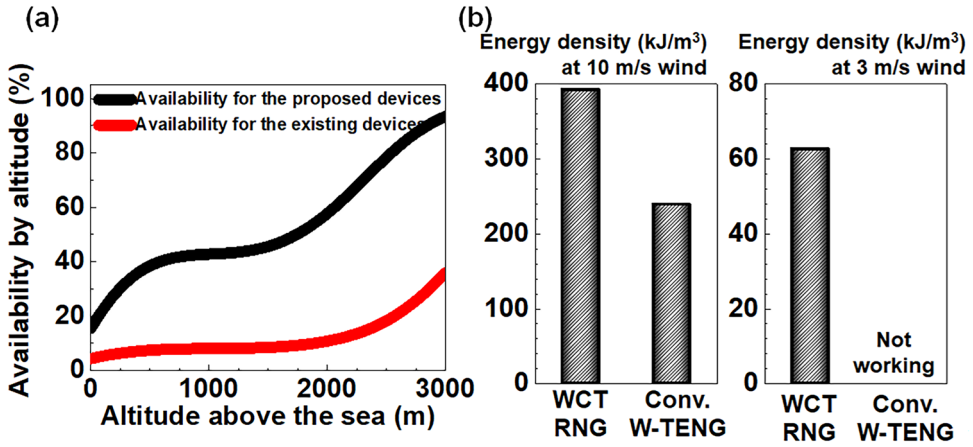

Figure 1. Comparison of the proposed WCT-RNG (experimental group) and conventional 4FW-TENG (control group II). (**a**) Compared availability between the proposed WCT-RNG and the conventional 4FW-TENG according to altitude above a sea level. (**b**) Compared histograms of estimated energy density at a wind velocity of 10 m/s and 3 m/s.

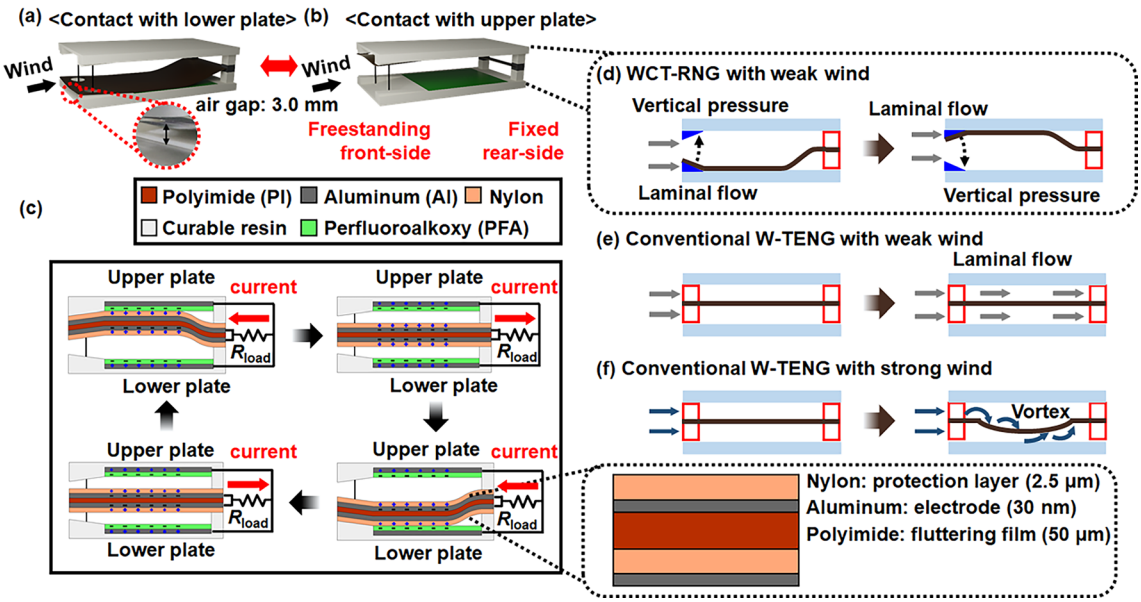

Figure 2. Schematic illustration of the proposed rear-fixed WCT-RNG for tilted and cross-sectional view. (**a**) Tilted view of the WCT-RNG where the fluttering film contacts the lower plate. (**b**) Tilted view of the WCT-RNG where the fluttering film contacts the upper plate. (**c**) Cross-sectional view of the WCT-RNG to show current flowing with a coupled mode that the WCT-RNG shares a common R_{load}. (**d**) Cross-sectional view of the WCT-RNG working with weak wind. (**e**) Cross-sectional view of the conventional W-TENG not working with weak wind. (**f**) Cross-sectional view of the conventional W-TENG working with strong wind.

Applied wind pressure

To evaluate output performances from the WCT-RNG under laboratory environments, a wind speed regulator (SUS316L EP regulator) accompanied with speed measurement equipment (VT 115 and TESTO 512) was used to control a wind pressure in a range of 6 psi to 70 psi, equivalent to 3.0–30.0 m/s, respectively.

Electrical measurements

The WCT-RNG was operated inside an aluminum shield box to screen out any external noisy electromagnetic field, which can influence on the output performances, such as randomness. The electrical outputs from the WCT-RNG were characterized using an electrometer Keithley 6514, which can directly measure electrical voltage and current with various ranges.

To evaluate long-term durability, a harsh wind velocity of 30 m/s was intentionally used for an acceleration test. For an acceleration test, we can intentionally impose harsh conditions. Nevertheless, the power harvested from stormy winds can be maintained even during natural and gentle breezes. It is important to note that the

power generated from wind is proportional to the cube of the wind speed (v^3)[18]. Therefore, the power output from the WCT-RNG under the condition of 30 m/s for 96 h can be comparable to that generated at 3 m/s for 10 years.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Results and discussion

The proposed WCT-RNG with a two-in-one configuration simultaneously acts as a power generator and TRNG, providing significant merits as an RNG and energy harvester. The capability of operating at low wind speeds has been dramatically improved over conventional methods. Among the aforementioned five security functions, 'availability' refers to the time-based probability that a target device is working properly at any given time, i.e., the working-time probability quantified with percentage. In Fig. S2, a detailed method is described to extract availability from statistical wind data. Availability can be a concern when an entropy source arises not from artificial means such as manufacturing-induced variability and operational-induced fluctuation, but from nature, such as wind. Even more concerning is when the wind is too weak or blows intermittently. The improved availability of the WCT-RNG in this work is attributed to the lowered working wind velocity: from 10 m/s, corresponding to a moderate gale, to 3 m/s, which is equivalent to natural wind. Wind energy varies according to various environments, and there are many statistical analyses in terms of wind speed and energy[19–22]. In conclusion, the average wind velocity can be statistically extracted according to the altitude above sea level in terms of spatial distribution. Conversely, in terms of time evolution, wind speed forms Weibull statistical distribution[23–25]; thus, the availability for the proposed WCT-RNG, whose operating condition is below 3 m/s, can be estimated. The 4FW-TENG (control group I), which works at a wind velocity of 10 m/s, was used as a primary reference[13].

Figure 1a compares the availability for the proposed WCT-RNG (experimental group) and the conventional 4FW-TENG (control group I) according to the altitude above sea level. For example, the working-time availability for the proposed WCT-RNG is 42% at 840 m, which is the world's average elevation[26,27]. This implies that the proposed WCT-RNG can generate energy and random numbers for 10 out of 24 h in a day. In contrast, the availability for the 4FW-TENG is 8% at 840 m, working only 2 out of 24 h. Thus, the working time for the proposed WCT-RNG is 5.2 times longer than that for the conventional 4FW-TENG. Figure 1b compares the extracted energy density for wind velocities of 10 m/s and 3 m/s. Specifically, it is defined as the harvested energy ($E_{\text{harvested}}$) divided by the total volume ($L{\cdot}W{\cdot}H_{\text{PLATE}}$). $E_{\text{harvested}}$ was estimated by $V_{\text{max}}{\cdot}I_{\text{max}}{\cdot}T_{\text{opr}}$, where V_{max} is maximal voltage, I_{max} is maximal current, and T_{opr} is operation time in a day. Here, both V_{max} and I_{max} were measured at load resistor (R_{load}) of 60 MΩ. Maximum power was extracted at R_{load} of 60 MΩ from a WCT-RNG device[14]. At 10 m/s, $E_{\text{harvested}}$ from the proposed WCT-RNG is 392.2 kJ/m^3 in a day, which is 1.6 times larger compared with $E_{\text{harvested}}$ from the 4FW-TENG. Even at 3 m/s, the WCT-RNG still produces 62.6 kJ/m^3 in a day; however, the conventional 4FW-TENG does not work at all. Therefore, the proposed WCT-RNG is superior to the conventional 4FW-TENG in terms of working-time availability and power generation.

Figure 2a,b are schematic illustrations of the WCT-RNG when the fluttering film is in contact with the lower plate and upper plate, respectively. As a shim, wedge-shaped protrusions were implemented to separate the fluttering film slightly from the resin plate so it can easily move up and down, even in a gentle breeze. Moreover, the wedge is also a favorable structure that redirects the lateral wind pressure to vertical force acting on the fluttering film; thus, the fluttering film can vertically move up after contact between the film and lower plate, as shown in Fig. 2a. With the same principle, the fluttering film vertically moves down after contact between the film and upper plate, as shown in Fig. 2b. Without these wedges, the fluttering film cannot move up and down because the film adheres to the upper or lower plate, which is illustrated in Fig. S4a.

When the bendable film flutters up and down, the surface of the nylon on the fluttering film is positively charged and the surface of the PFA on the resin plate is negatively charged via contact electrification[28,29]. The upper TENG unit creates electrical power when the fluttering film contacts and separates from the upper plate via electrostatic induction. Specifically, electrical current flows from the electrode of the upper plate to the upper electrode of the fluttering film when the film comes into contact with the upper plate. Conversely, when the film separates from the upper plate, electrical current flows from the upper electrode of the fluttering film to the electrode of the upper plate. The lower TENG unit also generates electrical power through the same principle that operates in the upper TENG unit.

Figure 2c exhibits the cross-sectional configurations of the WCT-RNG while describing the transient electrical voltage and current behaviors according to the movement of the fluttering film, like one period of a sine wave, as shown in Fig. S3a. This is because the fluttering film has two fixed ends. In contrast, the fluttering film of the 4FW-TENG moves like a quarter period of a sine wave owing to the end structure of the fluttering film, i.e., the curved shape of the fluttering film by wind is just concave or convex, as shown in Fig. S3b. Thus, the 4FW-TENG has a single unit unlike the double unit in the WCT-RNG.

As long as a chaotic wind is introduced to a gap of the WCT-RNG, the fluttering film contacts the upper plate then the lower plate iteratively or vice versa. When the fluttering film contacts the upper plate, current flows from the upper plate to the fluttering film through R_{load}. Afterwards, as they are far apart from each other, current flows reversely from the fluttering film to the upper plate through the R_{load}. Thereafter, the fluttering film contacts the lower plate, and in turn, current flows from the lower plate to the fluttering film through the R_{load}. Then, when they are separated, current reversely flows from the fluttering film to the lower plate through the R_{load}. Thus, the WCT-RNG inherently has a pair of electrodes: an upper TENG and a lower TENG that are connected in parallel. Each fluttering motion from each TENG cannot be identical due to turbulent wind in the gap that is continuously changing from time to time, even though the two TENGs are the same as each other. Consequently, the simple arithmetic sum of each open-circuit voltage (V_{OC}) from each decoupled TENG (control group II) cannot

be identical to the total V_{OC} from the coupled TENGs, as compared in Fig. 5d,e. They may appear similar at first glance, however, they are different upon closer inspection. Herein, V_{OC} refers to the electrical potential value where the resistance value of the load is infinite. This chaotic coupling can make an auto-correlation coefficient (R_{XX} (t_1,t_2)) between times t_1 and t_2 rapidly decrease to 0; thus, it can improve the randomness of a set of generated random numbers, as explained later.

Figure 2d describes the movement of the film in the WCT-RNG, even for a gentle breeze. The protruded wedges redirect wind flow, thereby making a laminar flow induce vertical pressure on the freestanding fluttering film. However, the relative dimension of the stoppers with a diameter of 0.5 mm is negligibly narrow compared to the plate width of 3 cm; thus, it cannot significantly influence the airflow near the wind inlet. Without the stoppers, the freestanding fluttering film can roll in due to strong wind input, as shown in Fig. S4b.

Figure 2e,f describe the movements of films in the conventional W-TENG (4FW-TENG) with weak wind and strong wind, respectively. Unlike the WCT-RNG working at a wind velocity of 3 m/s, the fluttering film of the 4FW-TENG was flipped up and flopped down when a strong wind velocity of 10 m/s was applied. This is because weak wind flow cannot produce vertical pressure to drive the film movement in the 4FW-TENG owing to the front-side fixed and rear-side freestanding structure[14]. Conversely, the proposed WCT-RNG produces vertical pressure from weak wind flow to activate film movement by the aid of the rear-fixed structure.

Figure 3a shows an optical photograph of the fabricated two-in-one WCT-RNG enclosing a TENG as well as an RNG and the assembled analog-to-digital converter (ADC) module. The generated AC-typed voltage from the fabricated WCT-RNG shown in Fig. 3b is converted into digital signals by the ADC module, as shown in Fig. 3c. An ADC-08100 evaluation module (EVM) was used to convert the analog-typed V_{OC} to digital random bits[30]. These converted digital bits are used as true random numbers. First, wind energy is converted to analog electrical voltage in the form of V_{OC} through the WCT-RNG. Second, the analog output V_{OC} is quantized and sampled to produce 8-bit digital signals. These digital signals are temporarily stored in memory devices in the processing unit. Finally, random data can be generated from this stored data whenever an end user requests random numbers[31,32]. In conclusion, the WCT-RNG module provides random numbers from wind energy, which can be used in cryptographic protocols that provide functions such as confidentiality, integrity, and authentication[33,34]. More specifically, a set of the generated true random numbers can be used as a cryptographic key and a cryptographic nonce during encrypting and decrypting operations to guarantee security confidentiality[35,36].

The directly measured V_{OC} from the fabricated WCT-RNG is shown in Fig. 4a. Figure S5a exhibits the schematic illustration for characterization of V_{OC} and measured V_{OC}, while Fig. S5b shows the schematic illustration for characterization of short-circuit current (I_{SC}) and measured transient I_{SC}. Its amplitude was 250 V at an input wind velocity (v_{in}) of 4 m/s, and its close-up view is shown in Fig. 4b. The transferred charge (Q_{TR}) was approximately 30 nC, which is extracted by integration of the measured I_{SC} with respect to time. Figure 4c–e display optical photographs and their corresponding schematics of the rear-fixed fluttering film in the manufactured WCT-RNG according to each peak position of V_{OC} in Fig. 4b. In one cycle period, there are three V_{OC} peaks. The highest V_{OC} peak is generated when the fluttering film is fully contacted to an electrode, as shown in Fig. 4c. The intermediate V_{OC} peak is created when the fluttering film is partially touching an electrode, as shown in Fig. 4d. The lowest V_{OC} peak is produced when the fluttering film is not in contact with the electrode, as shown in Fig. 4e. The V_{OC} with 3 peaks from the WCT-RNG looks like much more irregular, as V_{OC} with a single peak

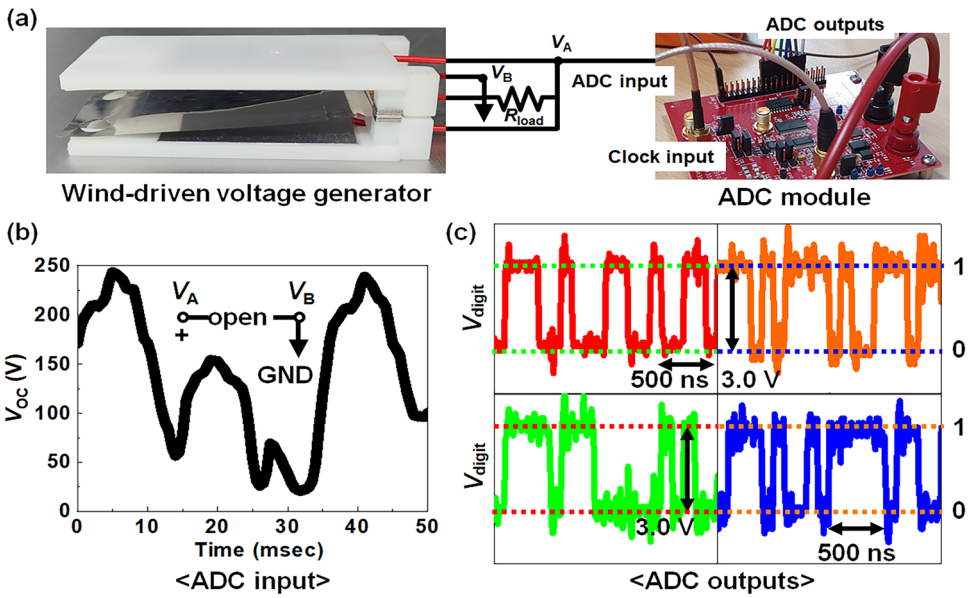

Figure 3. Configuration of 100% hard-ware based TRNG and its electrical outputs. (**a**) Optical photograph of manufactured WCT-RNG connected with an analog-to-digital converter (ADC) hardware (ADC-08100) module. (**b**) Measured analog output voltage (open-circuit voltage, V_{OC}) from the WCT-RNG at a wind pressure of 8 psi (4 m/s). (**c**) Measured digital output voltage (V_{digit}) from 4 pins of the ADC module for each digital pin.

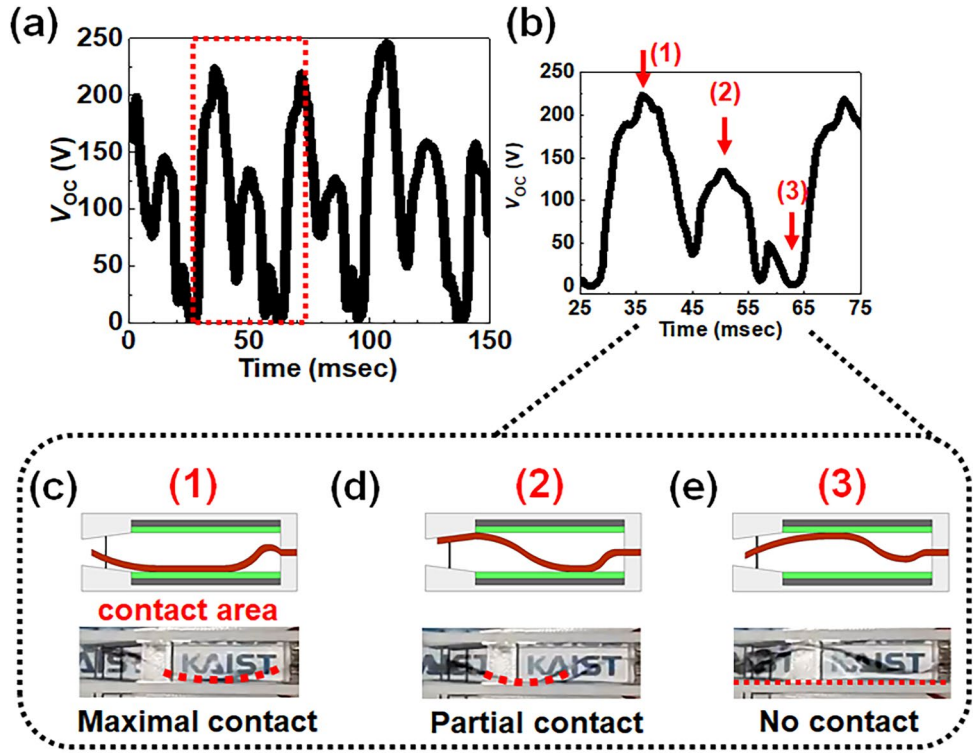

Figure 4. Measured V_{OC} with 4 m/s wind velocity at different contact positions. (**a**) V_{OC} extracted from the WCT-RNG. (**b**) Close-up view of the V_{OC} for the red box in (**a**). (**c**) Cross-sectional schematic and its optical photograph showing maximal contact, (**d**) showing no contact, and (**e**) showing partial contact.

from the 4FW-TENG is like a half cycle of a sine wave[13,37]. In conclusion, the WCT-RNG generates a V_{OC} that exhibits more irregular amplitude with atypical periodicity compared with the 4FW-TENG.

Figure 5 compares the electrical characteristics between the decoupled and coupled RFW-TENGs. While the decoupled RFW-TENG is a control group II, the coupled RFW-TENG is an experimental group, i.e., the WCT-RNG. In the decoupled RFW-TENG, the upper and lower TENG unit independently generates energy through the R_{load}. Thus, the experimental data of control group II shows two different periodic signals of V_{OC}, which can be superimposed later.

Figure 5a shows a schematic illustration of the decoupled TENG between the upper and lower TENG, which has its own R_{load}. Each TENG unit independently generates each V_{OC} through the separated R_{load}. In contrast, Fig. 5b depicts a schematic of the coupled TENG between the upper and lower TENG, which share a single R_{load}. As the fluttering film moves up and down like a sine wave, both TENGs produce jointed V_{OC} via the common R_{load}. Figure 5c exhibits a graph superimposing one V_{OC} from the upper TENG and the other V_{OC} from the lower TENG. However, Fig. 5d displays the arithmetically summed V_{OC} from the graph of Fig. 5c. The parallel connection of each decoupled TENG can make an arithmetic superposition of both outputs from the upper and lower TENG. A peak of the V_{OC} from the lower TENG is higher than that from the upper TENG due to downward gravitational force. Furthermore, Fig. S6 compares the measured V_{OC} for the upright RFW-TENG and the reversed RFW-TENG when used as an upside-down structure which verifies that the difference in the V_{OC} peak between them is attributed to gravitational force.

Conversely, Fig. 5e shows the directly measured V_{OC} from the coupled RFW-TENG through the shared R_{load} from the graph of Fig. 5c. In the case of the decoupled mode, the arithmetic sum between each TENG is evaluated after the calibration with an intentionally coherent phase, allowing for a direct comparison with the measured signals. Even though the overall waveform of Fig. 5d is similar to that of Fig. 5e, they are not the same upon careful examination. The similarity between Fig. 5d and e indicates that the total V_{OC} of the RFW-TENG is composed of each V_{OC} from the upper and lower TENG, and there are three notable features. First, the V_{OC} for both the upper and lower TENG possess periodic characteristics with approximated time intervals of 40 ms. Second, the V_{OC} measured from both the upper and lower TENG has complementary characteristics, meaning the time intervals to show peak voltage do not overlap. In other words, the high-voltage regions between the black line and red line in Fig. 5c do not overlap due to the fluttering film hitting the upper and lower TENG in rotation. Third, each amplitude of the V_{OC} from the upper TENG and the lower TENG is slightly different due to the intrinsic structure, where the contact force is stronger when the fluttering film goes to the lower unit than the upper unit by downward gravitational force. Figure 5f shows the amount of Q_{TR} per second from wind energy. The summation of each Q_{TR} from each decoupled TENG is the same as the measured Q_{TR} from the coupled TENGs, even though the amplitude and period of the V_{OC} are not identical. In conclusion, the signal of proposed WCT-RNG devices is composed of two V_{OC}. One is from the upper TENG and the other is from the lower TENG. It

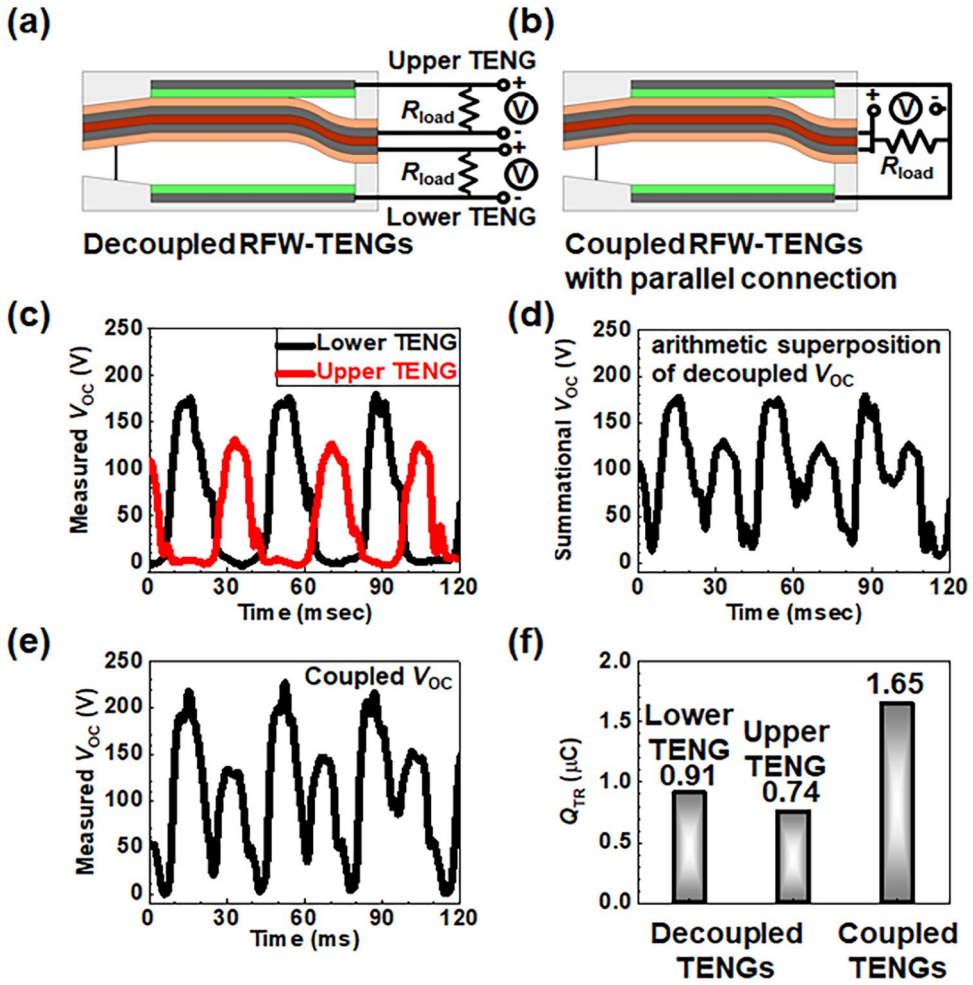

Figure 5. Cross-sectional schematics of the decoupled and coupled RFW-TENG and their characteristics. (**a**) Decoupled RFW-TENG (control group II) composed of the upper and lower TENG that have their own separated R_{load}. (**b**) Coupled RFW-TENG (experimental group) comprised of the upper and lower TENG that shares a common R_{load}. (**c**) Superimposed V_{OC} from the lower unit (black) and the upper unit (red) in the decoupled mode. (**d**) Arithmetically summed V_{OC} from the lower unit (black) and the upper TENG (red) in the decoupled mode. (**e**) Measured V_{OC} directly from the coupled RFW-TENG. (**f**) Comparison of Q_{TR} from the upper and lower TENG of the decoupled RFW-TENG and the coupled RFW-TENG.

should be noted that the coupled V_{OC} through a common electrical load is more random compared with each V_{OC} via a separated electrical load.

Figure 6a,b show the normalized amplitude after the discrete Fourier transform (FT) of the V_{OC} from a time domain to frequency domain for the decoupled and coupled RFW-TENGs, respectively[38,39]. Figure 6a shows the output results of the FT according to the frequency on the lower TENG (red line) and upper TENG (black line) in the case of the decoupled RFW-TENG. Conversely, Fig. 6b denotes the output results of the FT in the case of the coupled RFW-TENG. All signals in Fig. 6a,b possess identical spectrum peaks: 27.5 Hz and 55.0 Hz. Conventional W-TENGs that operate only at high velocity wind exhibit electrical signals with characteristics of a single-frequency system[13,37]. Thus, the signals that conventional W-TENGs produce are modeled as sinusoidal waves that possess Gaussian noise distribution for amplitude and frequency[13]. A single-frequency system is represented as $S = A_0 \cdot \cos(2\pi \cdot f_0 \cdot t)$, where A_0 is the amplitude of the cosine signal, f_0 is the frequency for a single frequency system, and t is the transient time. However, the proposed RFW-TENG, which operates under low-velocity wind conditions, possesses a dual frequency system with dual peak frequencies of 27.5 (=55.0/2) Hz and 55.0 Hz. These frequencies indicate that the measured transient signals are approximately represented to $S = A_1 \cdot \cos(2\pi \cdot 55t/2) + A_2 \cdot \cos(2\pi \cdot 55t)$, where A_1 is the amplitude of the cosine signal with 27.5 Hz, A_2 is the amplitude of the cosine wave with 55.0 Hz, and t is the transient time. Figure S7 shows the supposition of the sinusoidal signal between the $f_1 = 27.5$ Hz and $f_2 = 55.0$ Hz. It can be inferred that the signals produced by the dual peak frequency system are more complex than those produced by the single-frequency system. The dual peak frequencies originate from the dual contacts between the fluttering film and each electrode during one cycle. Figure S3a shows a snap-shot photograph of the fluttering film contacting the upper plate twice per cycle. Figure S3b displays a snap-shot photograph of the film of conventional W-TENG contacting the upper plate once per cycle. Due to

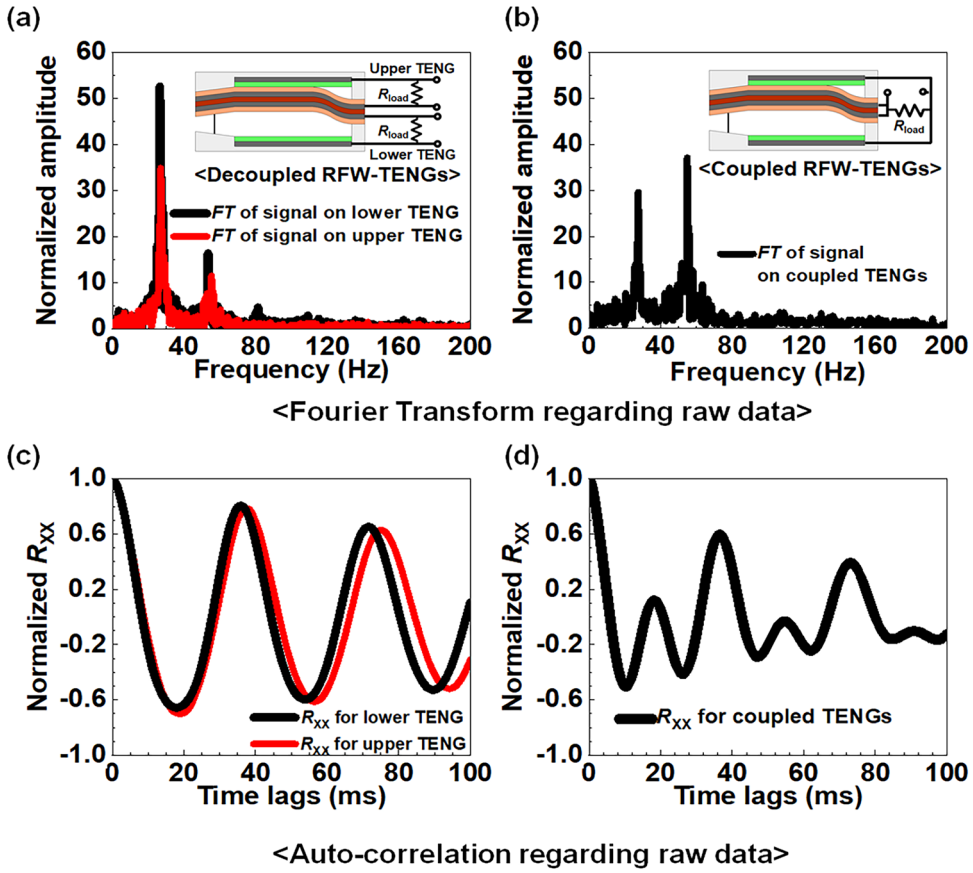

Figure 6. Comparison of discrete Fourier transform (FT) data and the auto-correlation coefficient (R_{XX}) between the decoupled mode and a coupled mode. (**a**) Superimposed FT spectrum of the measured V_{OC} from the lower (black line) and upper TENG (red line) of the decoupled RFW-TENG (control group II). (**b**) FT spectrum of the measured V_{OC} from the coupled RFW-TENG (experimental group). (**c**) Superimposed R_{XX} of the measured V_{OC} from the lower (black line) and upper TENG (red line) of the decoupled RFW-TENG. (**d**) R_{XX} of the measured V_{OC} from the coupled RFW-TENG.

these multiple contacts, the proposed WCT-RNG possesses a smooth fluttering movement in the fluttering film, unlike than that of conventional W-TENG, which is supported by Fig. S3a,b.

Figure 6c,d represent the auto-correlation coefficient (R_{XX}) of the decoupled RFW-TENG and the coupled RFW-TENG, respectively. The R_{XX} refers to the self-similarity of the signal over different delay times, i.e., the correlation of a signal with a delayed copy of itself as a function of delay[40]. Because it is useful to know how many repeating patterns there are, the R_{XX} can be a well-known parameter to visually estimate randomness[41]. The R_{XX} ranges from − 1 to 1. A high correlation of the $|R_{XX}|$ close to 1 indicates a uniform signal, whereas a low correlation of the $|R_{XX}|$ close to 0 presents a non-uniform and atypical signal, i.e., no correlation between two values of the same variable but at different times[42]. The R_{XX} shown in Fig. 6d reduces more rapidly than that in Fig. 6c according to time lag. The rapid reduction indicates that there is no relationship with a self-delayed signal[43,44]. Thus, the coupled RFW-TENG produces random numbers with improved randomness compared to the decoupled RFW-TENG. Therefore, from a TRNG point of view, the WCT-RNG is superior to both the decoupled RFW-TENG (control group II) and the previously reported 4FW-TENG (control group I)[13,37].

Table 1 compares the pass rate for each sub-suite test of the NIST SP 800-22 B for the evaluation of randomness[45,46]. The pass rate refers to the probability the test sequence satisfying the condition of a p-value $\geq \alpha$ (significance value), while the significance level of α was set to 0.01. A recommended significance value by NIST ranges from 0.001 to 0.01[46]. To evaluate randomness for all 15 sub-suite tests, a bit stream of 4,000,000 bits was directly extracted from the ADC module connected with the WCT-RNG. It shows an excellent pass rate of over 98% for all sub-suite tests. Conversely, the decoupled RFW-TENG (control experiment) exhibits a relatively low randomness. The average pass rate for the lower and upper TENG was 75.0 and 72.0, respectively. The complex electrical signals of WCT-RNG, originating from dual frequency characteristics with various noise frequencies and low correlation characteristics according to time lags, improve pass rate. In conclusion, the signal of the proposed WCT-RNG generates high-quality random numbers even when a low-velocity wind flow is applied.

Figure 7a compares the transient electrical signals between a fresh WCT-RNG and an aged WCT-RNG after undergoing intentional iterative stresses. To confirm the durability of the manufactured WCT-RNG, repeated cyclic stresses of 10^7 were intentionally applied with a wind pressure of 70 psi, which is equivalent to 30 m/s:

Pass rate (%)	4,000,000 bits (significance = 0.01)		
	Decoupled RFW-TENGs		
	Lower TENGs	Upper TENGs	WCT-RNG
Frequency	91	78	98
Frequency within a block	100	100	100
Runs	93	93	99
Longest run of ones	90	95	98
Binary matrix rank	99	99	100
Discrete Fourier transform	89	89	100
Serial	85	0	98
Approximate entropy	99	0	100
Cumulative sums	89	0	99
Non-overlapping template	0	100	100
Overlapping template	0	77	100
Maurer's universal statistics	0	98	100
Linear complexity	100	76	100
Random excursions	90	75	100
Random excursions variation	100	100	100
Average	75.0	72.0	99.5

Table 1. Comparison of each pass rate for all 15 test suites of the NIST SP 800-22 B for the decoupled mode (control group II) and WCT-RNG (experiment group).

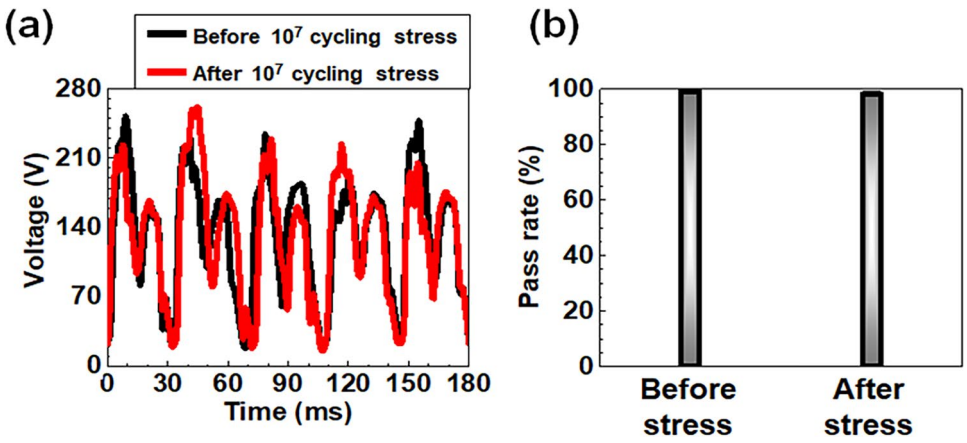

Figure 7. Comparison of TRNG performances in terms of durability. (**a**) Comparison of measured V_{out} from the RFW-TENG with a wind pressure of 8 psi (4 m/s) before and after cyclic stress of 10^7 under an air pressure of 70 psi (30 m/s). (**b**) Comparison of average pass rate for the 9 brief test suites of the NIST SP 800-22 B between a fresh WCT-RNG and an aged WCT-RNG.

comparable to the velocity of hurricanes and typhoons corresponding to Beaufort force level-12[47,48]. This harsh stress condition was used for an accelerated test to reduce the evaluation time of the durability within a short time. There was no degradation in the transient voltage even after cyclic stress. Figure 7b compares the averaged pass rate for the case of before stress and after stress. The pass rate was evaluated with a relatively shortened bit stream to further reduce the assessment time according to the 9 brief test suites of NIST SP 800-22 B[45,46]. The averaged pass rate was 99.5% for both cases and was unaffected even after the number of cyclic stresses up to 10^7. We conclude that the proposed WCT-RNG can reliably work as an RNG against mechanical durability.

Conclusion

We demonstrated a 100% hardware-based wind-driven cryptographic triboelectric random number generator (WCT-RNG) that utilizes a gentle breeze as an entropy source. This WCT-RNG consists of both an upper and a lower TENG, making it a two-in-one device as it serves as both an energy harvester and a true random number generator. Notably, the generated random numbers exhibited higher levels of randomness when the upper and lower TENG were in the coupling mode compared to the decoupling mode. In terms of randomness, the manufactured WCT-RNG exhibited a pass rate of 99.5% across all 15 test suites of the NIST SP 800-22B at 4 m/s. In terms of endurance, it maintained a 99.5% pass rate for the 9 brief tests of the NIST SP 800-22B, even after

enduring 10^7 iterative stresses at 30 m/s, which is equivalent to the stress of 3 m/s over a period of 10 years. Practicality can be further enhanced by integrating various components used in the current work into a single entity. This approach can pave the way for the development of self-powered and self-security functions in the era of IoT.

Data availability

The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Received: 11 September 2023; Accepted: 11 January 2024
Published online: 16 January 2024

References

1. Zhang, P. *et al.* Toward wisdom-evolutionary and primitive-concise 6G: A new paradigm of semantic communication networks. *Engineering* **8**, 60–73 (2022).
2. Soni, D. & Kumar, N. Machine learning techniques in emerging cloud computing integrated paradigms: A survey and taxonomy. *J. Netw. Comput. Appl.* **103**, 419 (2022).
3. Rey, V., Sánchez, P. M. S., Celdrán, A. H. & Bovet, G. Federated learning for malware detection in IoT devices. *Comput. Netw.* **204**, 108693 (2022).
4. Li, M., Guan, Q., Li, C. & Saiz, E. Self-powered hydrogel sensors. *Device* **1**, 100007 (2023).
5. Chang, J. *et al.* A dragonfly-wing-like energy harvester with enhanced magneto-mechano-electric coupling. *Device* **1**, 100021 (2023).
6. Yang, X., Xiang, C. & Wang, R. Harvesting clean energy from moisture. *Device* **1**, 100016 (2023).
7. SonicWall Inc. 2022 SonicWall cyber threat report. 2022. https://www.sonicwall.com. Accessed January 2023.
8. Karakaya, A., & Akleylek, S. A survey on security threats and authentication approaches in wireless sensor networks. In *2018 6th international symposium on digital forensic and security,* 1–4 (2018).
9. Epishkina, A., & Kogos, K. Quantum random number generator for secure communications. In *2016 International Siberian Conference on Control and Communications* 1–4 (2016).
10. Pain, P., Das, K., Sadhu, A., Kanjilal, M. R. & De, D. Novel true random number generator based hardware cryptographic architecture using quantum-dot cellular automata. *Int. J. Theor. Phys.* **58**, 3118–3137 (2019).
11. Kim, S. *et al.* Low-power true random number generator based on randomly distributed carbon nanotube networks. *IEEE Access* **9**, 91341–91346 (2021).
12. Kim, G. *et al.* Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor. *Nature Commun.* **12**, 1–8 (2021).
13. 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* **78**, 105275 (2020).
14. Tcho, I.-W. *et al.* A flutter-driven triboelectric nanogenerator for harvesting energy of gentle breezes with a rear-fixed fluttering film. *Nano Energy* **98**, 107197 (2022).
15. Bui, V. T. *et al.* Honeycomb-patterned polyimide-based triboelectric nanogenerator with excellent thermal stability and enhanced electrification performance. *ACS Appl. Energy Mater.* **5**, 9791–9800 (2022).
16. Ryan, J. J., Casalini, R., Orlicki, J. A. & Lundin, J. G. Controlled release of the insect repellent picaridin from electrospun nylon-6, 6 nanofibers. *Polym. Adv. Technol.* **31**, 3039–3047 (2020).
17. Yang, Z. *et al.* Strain-durable high-conductivity Nylon-6 fiber with 1D nanomaterial lamellar cladding for massive production. *ACS Appl. Mater. Interfaces* **13**, 57759–57767 (2021).
18. Kishorea, S. N., Rao, T. V. & Kumar, M. L. S. D. Fabrication and performance evaluation of savonious vertical axis wind turbine for uncertain speed regions. *Int. J. Thermal Environ. Eng.* **13**, 107–111 (2016).
19. Shoaib, M., Siddiqui, I., Rehman, S., Khan, S. & Alhems, L. M. Assessment of wind energy potential using wind energy conversion system. *J. Clean. Prod.* **216**, 346–360 (2019).
20. Rehman, S., Natarajan, N., Vasudevan, M. & Alhems, L. M. Assessment of wind energy potential across varying topographical features of Tamil Nadu, India. *Energy Explor. Exploit.* **38**, 175–200 (2020).
21. Lackner, M. A., Rogers, A. L., Manwell, J. F. & McGowan, J. G. A new method for improved hub height mean wind speed estimates using short-term hub height data. *Renew. Energy* **35**, 2340–2347 (2010).
22. Bañuelos-Ruedas, F., Angeles-Camacho, C. & Rios-Marcuello, S. Analysis and validation of the methodology used in the extrapolation of wind speed data at different heights. *Renew. Sustain. Energy Rev.* **14**, 2383–2391 (2010).
23. Wadi, M. & Elmasry, W. Statistical analysis of wind energy potential using different estimation methods for Weibull parameters: A case study. *Electr. Eng.* **103**, 2573–2594 (2021).
24. Ozay, C. & Celiktas, M. S. Statistical analysis of wind speed using two-parameter Weibull distribution in Alaçatı region. *Energy Convers. Manag.* **121**, 49–54 (2016).
25. Kidmo, D. K., Danwe, R., Doka, S. Y. & Djongyang, N. Statistical analysis of wind speed distribution based on six Weibull Methods for wind power evaluation in Garoua. *Cameroon, Revue des Energies Renouvelables* **18**, 105–125 (2015).
26. Orhan, O., Bilgin, U., Cetin, E., Oz, E. & Dolek, B. E. The effect of moderate altitude on some respiratory parameters of physical education and sports' students. *J. Asthma* **47**, 609–613 (2010).
27. Hare, V. J., Loftus, E., Jeffrey, A. & Ramsey, C. B. Atmospheric CO2 effect on stable carbon isotope composition of terrestrial fossil archives. *Nat. Commun.* **9**, 1–8 (2018).
28. Kang, H. *et al.* Metal nanowire–polymer matrix hybrid layer for triboelectric nanogenerator. *Nano Energy* **58**, 227–233 (2019).
29. Zhang, R. *et al.* All-inorganic triboelectric nanogenerators based on Mo6S3I6 and indium tin oxide. *Nano Energy* **89**, 106363 (2021).
30. Texas Instruments, ADC08100 Evaluation module user's guide. https://www.ti.com/tool/ADC08100EVM (2017).
31. Guan, L., Liu, P., Xing, X., Ge, X., Zhang, S., Yu, M., & Janger, T. Trustshadow: Secure execution of unmodified applications with arm trustzone. In *15th Annual International Conference on Mobile Systems, Applications, and Services,* 488–501 (2017).
32. Benhani, E. M., Bossuet, L. & Aubert, A. The security of ARM TrustZone in a FPGA-based SoC. *IEEE Trans. Comput.* **68**, 1238–1248 (2019).
33. Mohammad, S., Rahman, M. M. M., Farahmandi, F. Required policies and properties of the security engine of an SoC. In *IEEE International Symposium on Smart Electronic Systems* 414–420 (2021).
34. Kornaros, G., Tomoutzoglou, O. & Coppola, M. Hardware-assisted security in electronic control units: Secure automotive communications by utilizing one-time-programmable network on chip and firewalls. *IEEE Micro* **38**, 63–74 (2018).
35. Farha, F., & Ning, H. Enhanced Timestamp Scheme for Mitigating Replay Attacks in Secure ZigBee Networks. In *2019 IEEE International Conference on Smart Internet of Things (SmartIoT),* 469–473 (2019).

36. Chen, C. M., Wang, K. H., Yeh, K. H., Xiang, B. & Wu, T. Y. Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications. *J. Ambient Intell. Hum. Comput.* **10**, 3133–3142 (2019).
37. Kim, M. S., Tcho, I. W. & Choi, Y. K. Strategy to enhance entropy of random numbers in a wind-driven triboelectric random number generator. *Nano Energy* **89**, 106359 (2021).
38. Borkowski, J., Mroczka, J., Matusiak, A. & Kania, D. Frequency estimation in interpolated discrete fourier transform with generalized maximum sidelobe decay windows for the control of power. *IEEE Trans. Ind. Inf.* **17**, 1614–1624 (2020).
39. Sun, S. *et al.* Shape characterization methods of irregular cavity using Fourier analysis in tunnel. *Math. Comput. Simul.* **187**, 191–214 (2021).
40. Berne, B. J., Boon, J. P. & Rice, S. A. On the calculation of autocorrelation functions of dynamical variables. *J. Chem. Phys.* **45**, 1086–1096 (1966).
41. Ma, X. *et al.* Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).
42. Hu, W. W., Wang, S. H. & Li, C. P. Gaussian integer sequences with ideal periodic autocorrelation functions. *IEEE Trans. Signal Process.* **60**, 6074–6079 (2012).
43. Baltagi, B. H., Song, S. H., Jung, B. C. & Koh, W. Testing for serial correlation, spatial autocorrelation and random effects using panel data. *J. Econ.* **140**, 5–51 (2007).
44. Diaz, F. Performance prediction using spatial autocorrelation. In *Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval,* 583–590 (2007).
45. Sulak, F., Uğuz, M., Kocak, O. & Doğanaksoy, A. On the independence of statistical randomness tests included in the NIST test suite. *Turk. J. Electr. Eng. Comput. Sci.* **25**, 3673–3683 (2017).
46. Georgescu, C. & Simion, E. New results concerning the power of NIST randomness tests. *Proc. Roman. Acad. Ser. A* **18**, 381–388 (2017).
47. Sparks, P. R. Wind speeds in tropical cyclones and associated insurance losses. *J. Wind Eng. Ind. Aerodyn.* **91**, 1731–1751 (2003).
48. Berger, G., Lacharpagne, J.-C., Velde, B., Beaufort, D. & Lanson, B. Kinetic constraints on illitization reactions and the effects of organic diagenesis in sandstone/shale sequences. *Appl. Geochem.* **12**, 23–25 (1997).

Acknowledgements

This work was supported by the National R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science (RS-2023-00260637, and RS-2023-00217888), BK21 FOUR (Connected AI Education & Research Program for Industry and Society Innovation, KAIST EE, No. 4120200113769), and the 2018 Open R&D project of the Korea Electric Power Corporation (KEPCO) (R18EO01). This research was supported by the research fund of Hanbat National University in 2023.

Author contributions

M.-S.K.: conceptualization, investigation, writing-original draft, software, visualization. I.-W.T.: former analysis, data curation, methodology, resources. Y.-K.C.: validation, writing-review and editing, supervision, project administration, funding acquisition.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-024-51939-2.

Correspondence and requests for materials should be addressed to Y.-K.C.