scientific reports

Check for updates

OPEN

# Analyses of unpredictable properties of a wind-driven triboelectric random number generator

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

**Wind-driven triboelectric nanogenerators (W-TENGs) are a promising candidate for an energy harvester because wind itself possesses unexhausted, ubiquitous, and clean properties. W-TENG has also been used as a random number generator (RNG) due to the inherent chaotic properties of wind that is also an entropy source. Thus, a W-TENG which simultaneously generates both power and true random numbers with a two-in-one structure, is a wind-driven RNG (W-RNG) like the Janus. However, a root cause of W-RNG unpredictability has not been elucidated. In this work, the unpredictability, which is essential and critical for an RNG, is statistically and mathematically analyzed by auto-correlation, cross-correlation, joint entropy, and mutual information. Even though the overall shape of the total output analog signals from the W-RNG looks like a sinusoidal wave that is not obviously unpredictable, discretized digital signals from the continuous analog output become unpredictable. Furthermore, partial adoption of 4-bit data from 8-bit raw data, with the aid of analog-to-digital converter hardware, further boosts the unpredictability. The W-RNG, which functions as a W-TENG, can contribute to self-powering and self-securing outdoor electrical systems, such as drones, by harvesting energy and generating true random numbers.**

Recently, the Internet of Things (IoT) technology has emerged as an innovative paradigm which attains hyper-connectivity of objects, devices, and people[1]. It is estimated that the number of connected devices will grow to 20 billion in the near future[2,3]. In IoT and smart system technology, each device must possess the ability to supply stable energy and to communicate with other devices[4]. Security functions such as confidentiality, integrity, availability, authentication, and non-repudiation are crucial for securing the communications among all connected devices[5–10]. A true random number generator (TRNG), which is one of the promising security primitives based on hardware, plays a significant role in supporting the aforementioned security functions. Thus, the development of a TRNG with a variety of entropy sources is vital to achieving secure IoT technology[11–15]. There were a few reports on devising a TRNG using various entropy sources in nature[16–18]. However, their extraction of true random numbers through post-processing can be a demerit in reducing power consumption. If possible, no use of post-processing is preferred.

Alternatively, a TRNG without post-processing was demonstrated with the aid of a prototyped wind-driven triboelectric nanogenerator (W-TENG)[19]. Their W-TENG based TRNG not only provides energy harvesting but also security functions for communicating systems *e.g.* IoT, a smart grid for an electricity network, and in-flight applications. It produces true random numbers by transferring chaotic wind flow to random electrical signals via triboelectrification. The random electrical signals produced from hardware with a wind entropy source are generated without any post-processing algorithms. The random signals from the W-TENG satisfy the requirements of the NIST SP 800-22B, which is the most widely used standard methodology to evaluate randomness. Previous works have reported that randomness is attributed to the chaotic behaviors of wind[20]. However, intensive and in-depth analyses regarding both the unpredictability of the output signals from the W-TENG and suitability as an entropy source remain insufficient from a theoretical and statistical point of view. It is now crucial to quantify the unpredictable properties to enhance the practicality of W-TENG based TRNG.

[1]School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea. [2]Department of Semiconductor System Engineering, Hanbat National University, 125 Dongseo-daero, Yuseong-gu, Daejeon 31538, Republic of Korea. ✉email: ykchoi@ee.kaist.ac.kr

In this work, we conducted in-depth analyses of the unpredictability and randomness of the generated random numbers from the W-TENG based TRNG. We examined auto-correlation, cross-correlation, joint entropy, and mutual information, ensuring distinctive security features such as confidentiality, integrity, availability, authentication, and non-repudiation. As a significant advancement compared to our previous work[19], we installed the W-TENG on a commercial drone, directly harvesting energy from the wind generated by the drone's rotating blades. We then used this harvested energy to power a light-emitting diode, effectively demonstrating the W-TENG's capability as an energy harvester. Moreover, our approach for extracting true random numbers diverged from traditional software-based methods reliant on virtual analog-to-digital converters (ADCs). Instead, we sourced these true random numbers directly from the hardware of an ADC connected to the W-TENG, thereby establishing a reliable and hardware-based random number generator. Consequently, the W-TENG based TRNG can contribute to securing and self-powering outdoor electrical systems by harvesting energy and generating true random numbers. Moreover, it can also enhance the security of smart power grids.

## Materials and methods

### Fabrication of wind-driven TENG

For this study, we fabricated another W-TENG with an enclosed thin flip-flop polytetrafluoroethylene (PTFE) film[19]. The thickness of the PTFE film is 0.2 mm. The PTFE film has a small gap between a top and a bottom electrode to guide air flow. This air gap ($h$) acts as an inducer to generate a chaotic vortex from inlet wind. The size of the Al electrodes is 40 mm in length × 40 mm in width, and its thickness is 1 mm[20]. To separate the top and bottom electrode, 4 spacers are employed at each corner of the W-TENG. Each spacer is composed of neodymium magnets, which are vertically stacked[21,22]. The size of the neodymium magnets is 5 mm in length × 5 mm in width, and its thickness is 0.5 mm. Because the size of the magnet spacer is small enough compared to the size of the electrodes, it cannot influence the wind vortex in the air-gap. In each corner, the PTFE film is fixed in between upper two magnets and lower two magnets. The air-gap distance between the top and bottom electrode becomes 2.2 mm because the sum of 0.5 mm × 4 magnets and 0.2 mm PTFE film is 2.2 mm.

### Applied wind pressure

Artificial wind was generated by an air gun with a regulator (SUS316L EP regulator), which is used to control the wind speed for a referenced test. The regulator controls wind pressure, which is ranged from 10 psi (4.3 m/s) to 30 psi (12.8 m/s). In all control experiments, unless specified otherwise in Fig. 7, the artificial wind was maintained at an inlet pressure of 30 psi (12.8 m/s). For actual experiments, a semi-natural wind generated by the rotating wings of a drone was utilized.

## Results and discussion

### Implementation of wind-driven triboelectric random number generator

Our manufactured W-TENG can simultaneously act as a power generator and a TRNG, with a two-in-one configuration like the Janus. Figure 1a shows the two-in-one type W-TENG mounted on a commercial drone. A light emitting diode (LED) is utilized as an optical indicator to assure that power is generated from the installed W-TENG during flight. Figure S1 exhibits the lighting of the LED, which signifies power generation from the W-TENG on the drone. For the actual experiments, the applied wind pressure to the W-TENG was driven by the rotating wings of the drone. Figure S1a shows the W-TENG with the LED mounted on the drone. It is known that wind pressure is maximal at the center of the drone, which has 4 rotary wings[23,24]; thus, the W-TENG with the LED was installed at the center of the drone. Figure S1b illustrates a brief electric circuit comprised of the W-TENG and the LED. Figure S1c shows an image of the lightened LED, and Fig. S1d displays the close-up view of the inset, denoted by the white dashed line. This figure compares LED images at the turned-on state (left column) and at the turned-off state (right column). As shown in Fig. 1b, in accordance with a purpose, an end user can employ an operational mode: a power generating mode for energy harvesting and an RNG mode for cryptographic communication. When the energy harvesting mode is enabled, the generated output signal is transformed to an electric charger in a drone as a power source for a TENG. When the RNG mode is activated, the analog output voltage signals are converted to 8-bit digital signals that are discretized by a sampling process via an ADC, as an entropy source for an RNG. Figure 1c shows that the LED was connected with two electrodes of the manufactured W-TENG and turned on solely by its generated electricity. For this in-door experiment, controlled wind was set to 30 psi, which is approximately 12.8 m/s, which produced 0.79 mW. The peak power of 0.79 mW was obtained by multiplying output voltage of 149 V and output current of 5.3 μA at resistance of 10 MΩ. Figure 1d shows the measured output voltage between $V_A$ and $V_B$ of Fig. 1b with respect to the time evolution. It resembles a sinusoidal wave; however, it is not actually a genuine sine wave. Such sine wave-like behavior is ascribed to the alternating flip-flop actuation of the thin PTFE film between the two electrodes. Pseudo-sine wave behavior, but with unpredictable randomness, is attributed to the chaotic wind vortex in the airgap. In the initial state, the thin PTFE film was located in the middle, which is in between the top and the bottom electrode. When wind is introduced to the small gap of the W-TENG, it flutters upwardly and downwardly between the two electrodes. Physical contact between the PTFE film and the aluminum electrode induces triboelectric effects, which generate electrical energy. Herein the electrical output signal is a continuous analog voltage arising from the iterative flip-flop of the PTFE film. Through the abovementioned ADC hardware, the analog voltage can be converted to a digital signal[25,26].

Figure 2a exhibits a photograph of an ADC-08100 evaluation module (EVM) for the conversion of the analog-to-digital[27]. In our previous works, such conversion was realized by use of Matlab in a software manner[19,20]. In contrast, the hardware-based data conversion in this work was conducted using the ADC-08100 EVM module mounted on a printed circuit board (PCB) with power consumption at a mW level, as a proof-of-concept for

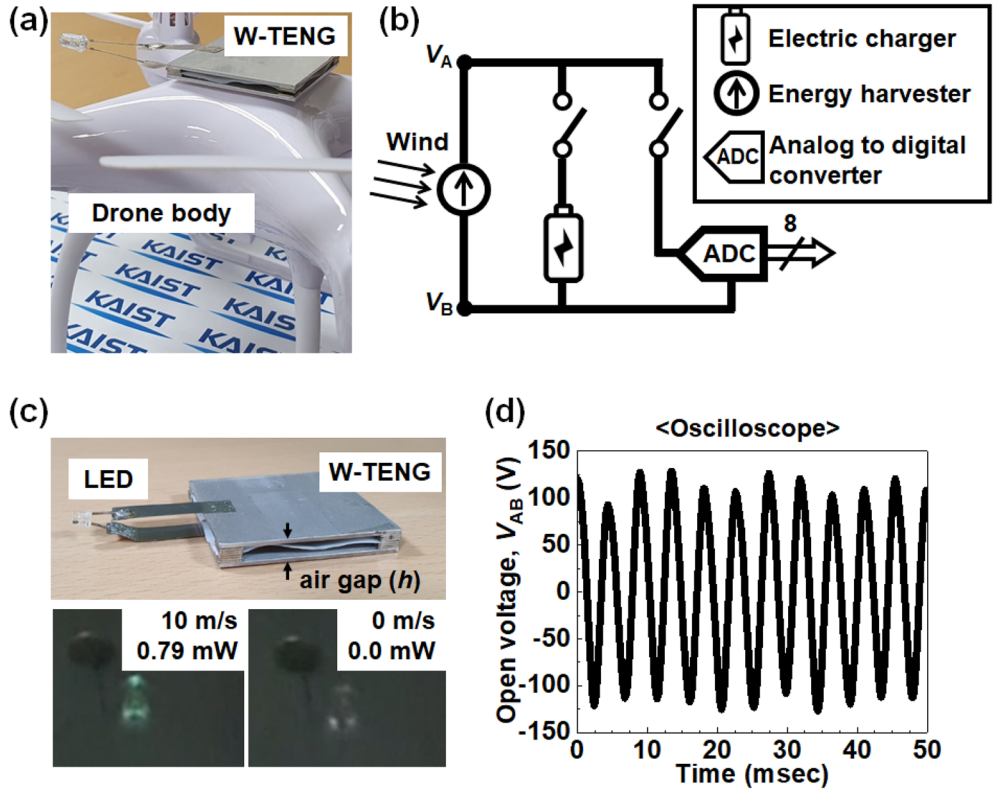


**Figure 1.** (**a**) Manufactured two-in-one type W-RNG mounted on a commercial drone. (**b**) Electrical configuration of the W-RNG, electric charger, and ADC. (**c**) Optical photographs of turned-on LED with a wind pressure of 30 psi (left) and turned-off LED with 0 psi (right). (**d**) Measured output voltage from the W-RNG with a wind pressure of 30 psi.

actual random number generation from a W-TENG based TRNG. Such a high level of power consumption is attributed to the extra power consumption of supportive components mounted on the same PCB such as a low-dropout voltage regulator, clock buffer, output buffer, and onboard crystal oscillator. If an ADC is dedicated to a W-TENG based TRNG and constructed as a type of system-on-chip (SoC), its power consumption can be reduced to less than 200 nW, as shown in Table S1[28–30]. In this work, each output pin corresponding to each digital output among the 8-bits is assigned as *bit-8*, *bit-7*, *bit-6*, and so on, in the ADC-08100 EVM. The *bit-8* signal refers to the most significant bit (MSB) signal, while the *bit-1* signal indicates the least significant bit (LSB) signal. Figure 2a shows the four conductive cables connected to the ADC output pins for *bit-4*, *bit-3*, *bit-2*, and *bit-1* signals among the 8-bit digital bits. Furthermore, each conductive cable is characterized by an oscilloscope. Figure 2b shows each waveform of the measured voltage from the *bit-4*, *bit-3*, *bit-2*, and *bit-1* signals through the ADC-08100 EVM. The measured *bit-4*, *bit-3*, *bit-2*, and *bit-1* signals are represented as green, blue, red, and purple, respectively. As shown in Fig. 2b, the voltage difference between the high-level and low-level output voltage is 3.0 V in the ADC-08100 EVM.

Herein, $DS_{n_{\mathrm{ADC}}}(t)$ is defined to show a transient digital state, where $n_{\mathrm{ADC}}$ is the number of the extracted bit among the 8 output bits in the ADC. It is represented as follows:

$$DS_{n_{\mathrm{ADC}}}(t) = \sum_{j=1}^{n_{\mathrm{ADC}}} 2^{j-1} \cdot b_j (n_{\mathrm{ADC}} = 1, \ldots, 8)$$

where $b_j$ is a bit value for a bit-$j^{\mathrm{th}}$ signal and $t$ is the time evolution. $DS_8(t)$ ranges from 0 to 255, while $DS_4(t)$ ranges from 0 to 15. The value of $b_j$ is '0' or '1'. For example, when the measured bits for each of the 8 bits are 1, 0, 1, 0, 1, 0, 1, and 1 in descending order at $t = 100$ µs, $DS_8(100\ \mu s)$ becomes 179 ($2^7 + 2^5 + 2^3 + 2^1 + 2^0$) and $DS_4(100\ \mu s)$ is 11 ($2^3 + 2^1 + 2^0$). Figure 2c represents the measured transient digital state of $DS_8(t)$ enclosing the 8 output bits and Fig. 2d denotes that of the $DS_4(t)$ including 4 output bits. The digitized state of the $DS_8(t)$ seems to follow a periodic and regular pattern like a sinusoidal wave. In contrast, the digitized state of the $DS_4(t)$ conforms to a sporadic and irregular pattern unlike a sinusoidal wave.

## In-depth analysis for unpredictability of random numbers

Figure 3a and b visualize the abovementioned regular and irregular properties, respectively, in the form of a 2-dimsensional contour map. Figure 3a exhibits a contour map from the measured $DS_8(t)$, while Fig. 3b displays that from the measured $DS_4(t)$. These contour maps are expressed in monotoned gray scale where a white and

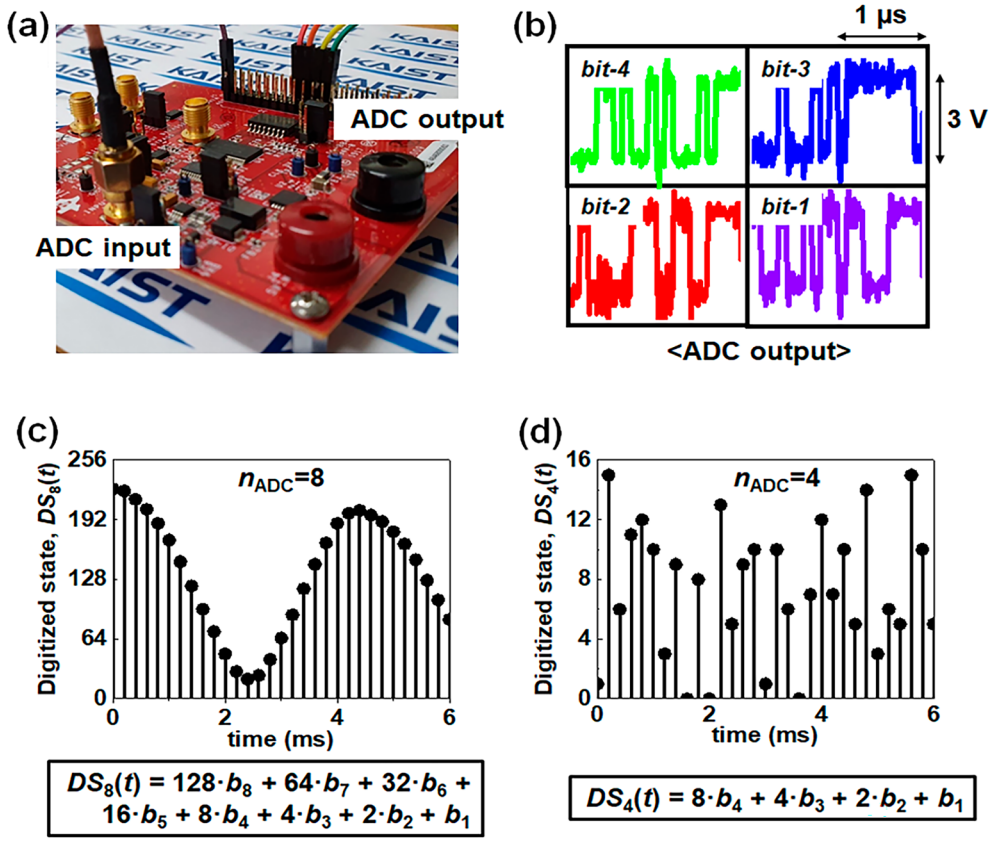


**Figure 2.** (**a**) Optical photograph of employed ADC test board with the ADC-08100 module. (**b**) Measured output voltage from the ADC test board for *bit-4*, *bit-3*, *bit-2*, and *bit-1*. (**c**) Measured discrete states of $DS_8(t)$ ranging from 0 to 255 for signals of *bit-8* to *bit-1*. (**d**) Measured digitized states of $DS_4(t)$ ranging from 0 to 15 for signals of *bit-4* to *bit-1*.

a black color indicate a value of high and low $DS_{n_{ADC}}(t)$, respectively. Each dot is filled according to a chronological order of the time evolution. The contour map of the $DS_8(t)$ shows a periodic and regular pattern, which was observed in the transient digital states of Fig. 2c. On the contrary, the contour map of the $DS_4(t)$ shows an irregular and noisy pattern, which was found in the transient digital states of Fig. 2d. Consequently, the transient digital states of the $DS_4(t)$ are more unpredictable than those of the $DS_8(t)$ from a graphical point of view. Thus, we can infer that partial adoption of ADC output bits significantly influences the unpredictability and randomness, *i.e.*, the lower bit such as LSB results in increased unpredictability. Figure S2 displays a contour map of the measured digitized state of the $DS_8(t)$ to the $DS_1(t)$ according to the number of the employed ADC bits.

Figure 3c and d compare a normalized probability density function of $DS_8(t)$ and $DS_4(t)$, respectively. Distribution of the original probability density extracted through the ADC hardware is normalized by the number of the digitized states, $2^{n_{ADC}}$. For example, $DS_8(t)$ is normalized by $2^8 = 256$, whereas $DS_4(t)$ is normalized by $2^4 = 16$. Thus, a value of 1 is ideal, which corresponds to perfect uniformity. Closer to 1 implies more unpredictability; thus, it is important to check whether the distribution of the digitized state is uniform or not. The distribution of $DS_8(t)$ is non-uniform, while that of $DS_4(t)$ is uniform. We conclude that $DS_4(t)$ is more unpredictable than $DS_8(t)$. Figure S3 displays the normalized distribution of the probability density for other digitized states, *e.g.*, $DS_7(t)$, $DS_6(t)$, $DS_5(t)$ and $DS_3(t)$. As $n_{ADC}$ decreases, the distribution of the probability density becomes more uniform, *i.e.*, more unpredictable.

Figure 4 shows the auto-correlation and cross-correlation of the extracted digital signals from the ADC digital outputs. The auto-correlation is quantified as a correlation coefficient ranging from − 1 to 1. Closer to 0 indicates less auto-correlation between two values of the same variable but at different times. The cross-correlation is also metrized as another correlation coefficient ranging from − 1 to 1. When the value approaches 0, it indicates that there is less cross-correlation between two variables as their values change at different times relative to each other. The auto-correlation coefficient can measure similarity between variables in an intra device and the cross-correlation coefficient can do the same in inter devices. It is rational to verify randomness and unpredictability by evaluating the auto-correlation and the cross-correlation[31–33]. When a value of the auto-correlation and the cross-correlation coefficient is close to 0, sequences of raw data are independent of each other, randomly distributed, and unpredictable[32].

The auto-correlation coefficient refers to the self-similarity within a single signal as a function of different delay times[34,35]. The auto-correlation is represented as follows:

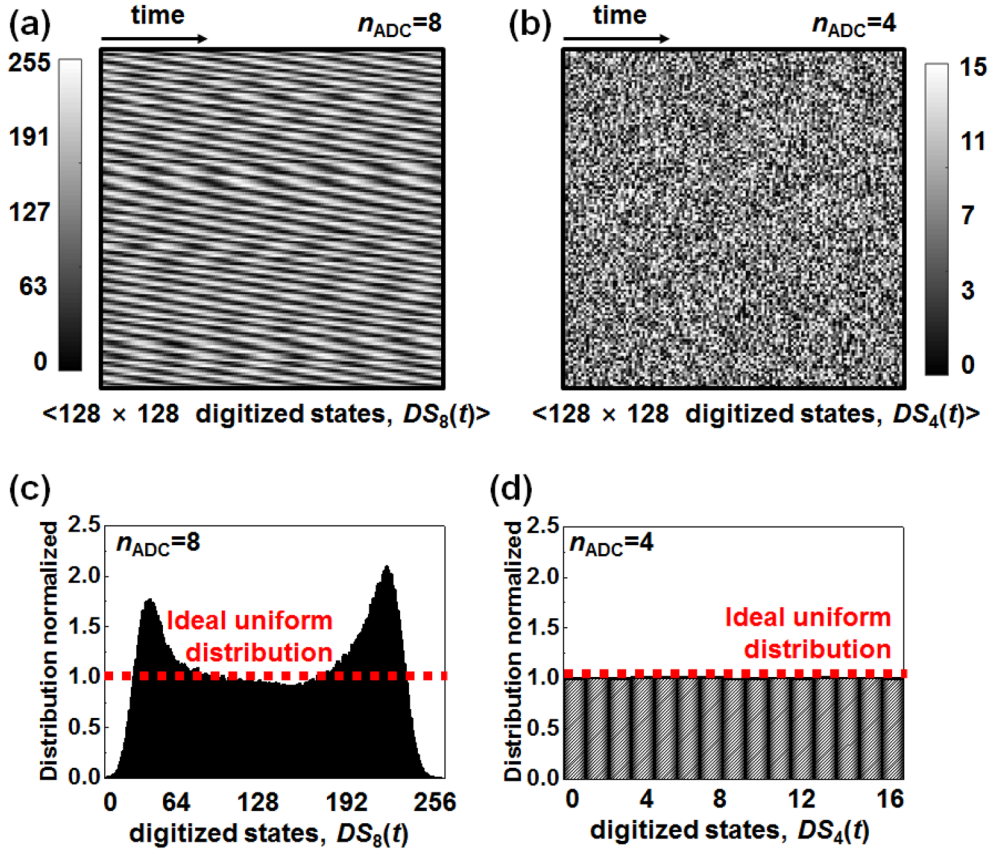


**Figure 3.** (**a**) Regular patterned contour map with measured digitized states of $DS_8(t)$ ranging from 0 to 255 when the number of the extracted ADC bit ($n_{ADC}$) is 8. (**b**) Irregular patterned contour map with measured digitized states of $DS_4(t)$ ranging from 0 to 15 when $n_{ADC}=4$. (**c**) Non-uniform probability density distribution of $DS_8(t)$ ranging from 0 to 255 when $n_{ADC}=8$. (**d**) Uniform probability density distribution of digitized states of $DS_4(t)$ ranging from 0 to 15 when $n_{ADC}=4$.

$$R_{XX}(\tau) = \frac{1}{|R_{XX}(0)|^2}\int_{-\infty}^{+\infty} x(t)x(t+\tau)dt.$$

All coefficients are normalized by $|R_{XX}(0)|^2$, which is the coefficient for no time lag. Thus, the auto-correlation coefficient of $R_{XX}(0)$ is always 1 by definition of the normalized auto-correlation function[35]. A correlation of -1 represents a perfectly negative correlation, while a correlation of 1 indicates a perfectly positive correlation. In contrast, a correlation of 0 refers to no linear relationship between the same variable at different times. This implies that random digital bits are unpredictable for the time evolution[36,37].

Figure 4a describes the method to extract the auto-correlation coefficient in an intra device. First, digital bits are generated from 8 output pins of the ADC hardware. Second, the sampling process is conducted at every 200 μs. Third, the digital bits are converted to $x(t)$ with a conversion rule of a logic value: switching of logic '0' to integer '− 1' and switching of logic '1' to integer '1'. From these procedures, $x(t)$ is extracted from the ADC hardware. This conversion makes a fair comparison of the auto-correlation coefficient[38]. Finally, the auto-correlation coefficient of $R_{XX}$ is extracted from $x(t)$ for each of digital output. Figure 4b exhibits the auto-correlation coefficient of *bit-8* according to time lag. Its coefficient of the *bit-8* shows periodicity. In other words, the digitized signals of the *bit-8* are predictable owing to the self-similarity for the time evolution. In contrast, the auto-correlation coefficient of *bit-4* and *bit-1* are very rapidly reduced to 0, which infers that there is no relationship with a self-delayed signal, as shown in Fig. 4c and d[36,37]. Figure S4 shows the other auto-correlation coefficients according to the ADC digital output signals from the ADC hardware for an intra device from *bit-8* to *bit-1*.

Figure 4e describes the method to extract the cross-correlation coefficient in inter devices. First, digital bits are generated from two arbitrary devices (e.g., device #1 and device #2) via the ADC hardware. Second, the generated digital bits are converted to discrete-time signals from continuous-time signals by the sampling process. Third, the converted signals are modulated to $x(t)$ (device #1) and $y(t)$ (device #2). A modulation rule of a logic value is switching of logic '0' to integer '− 1' and switching of logic '1' to integer '1'. Finally, the cross-correlation coefficient of $R_{XY}$ is extracted from $x(t)$ and $y(t)$. The cross-correlation coefficient between inter devices is expressed as follow:

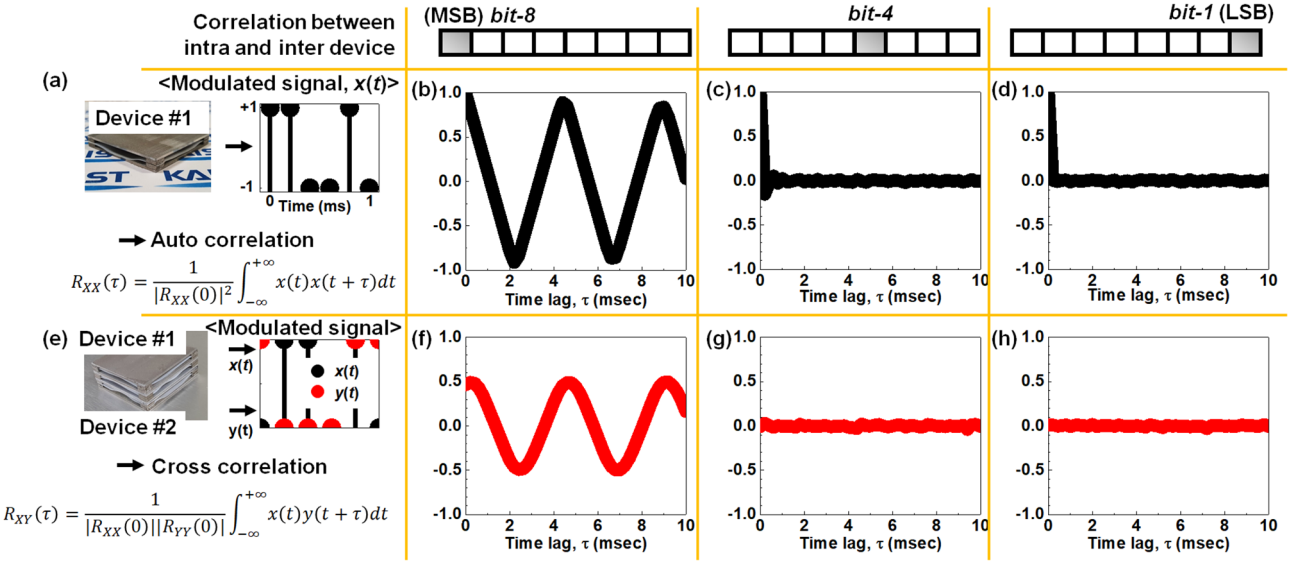


**Figure 4.** Analyses of predictability in terms of auto correlation for an intra device and cross correlation for inter devices. (**a**) Extraction of auto correlation for an intra device. (**b**) Coefficient of auto correlation for the signal of *bit-8* according to time lag. (**c**) Coefficient of auto correlation for the signal of *bit-4* according to time lag. (**d**) Coefficient of auto correlation for the signal of *bit-1* according to time lag. (**e**) Extraction of cross correlation between inter devices. (**f**) Coefficient of cross correlation for the signal of *bit-8* according to time lag. (**g**) Coefficient of cross correlation for the signal of *bit-4* according to time lag. (**h**) Coefficient of cross correlation for the signal of *bit-1* according to time lag.

$$R_{XY}(\tau) = \frac{1}{|R_{XX}(0)||R_{YY}(0)|}\int_{-\infty}^{+\infty} x(t)y(t+\tau)dt.$$

All coefficients are normalized by $|R_{XX}(0)||R_{YY}(0)|$, which is the multiplication product between two auto-correlation coefficients for no time lag. A correlation of − 1 represents a perfectly negative correlation and a correlation of 1 denotes a perfectly positive correlation. In contrast, a correlation of 0 indicates that there is no linear relationship between the $x(t)$ and $y(t)$ variables. Even though $x(t)$ is known, $y(t)$ cannot be predicted from the known $x(t)$ due to the inherent device-to-device randomness[39,40]. Figure 4f exhibits the cross-correlation coefficient of *bit-8* according to time lag. Its coefficient of *bit-8* is periodic, which resembles the auto-correlation coefficient, as shown in Fig. 4b; however, the cross-correlation coefficient of *bit-4* and *bit-1* becomes 0, as shown in Fig. 4g and h. This implies that there is no relationship between the inter-device signals. Figure S5 exhibits the other cross-correlation coefficients from the ADC hardware for inter devices from the *bit-8* to *bit-1* signals. Through analyses of the correlations between intra- and inter-devices, the lower $n_{ADC}$ extracted from outputs of the ADC hardware results in increased unpredictability, which is attractive for the improvement of true random number quality.

A Markov chain provides a method to analyze uncertainty and unpredictability through simple matrix calculations[41–43]. In particular, the value of joint entropy and mutual information can be extracted from a Markov chain model, which are mathematical and statistical methods to quantify unpredictability. In Fig. 5, the Markov chain model is visualized for an intra device and inter devices. Their distributions, according to the time evolution, are illustrated in Fig. 5a. Conversely, Fig. 5b describes methods to extract Markov chains for inter devices. Two types of transitions are available. One is a time transition between $X(t = T_i)$ and $Y(t = T_{i+1})$ for an intra device. $T_i$ is a time that an ith sampling process is performed, whereas $T_{i+1}$ is another time that an $(i+1)^{th}$ sampling process is conducted. For example, the time transition is investigated between $t = T_i$ and $t = (T_i + 200\ \mu s)$ with a sampling rate of 200 µs, as shown in Fig. 5a. The other is a spatial transition between device #1 and device #2 for the inter devices, as described in Fig. 5b. In other words, the spatial transition is investigated between a digitized state of device #1 and device #2 under an identical time condition, $t = T_i$. As shown in Fig. 5c, the Markov chain model is represented with a probability density function of $P(X,Y)$ as the matrix form. Its elements are $P_{(1,1)}$, $P_{(1,2)}$, ⋯ , and $P_{(N,N)}$. The probability density function of $P(X,Y)$ is also called the joint probability distribution regarding two random variables $X$ and $Y$. $N$ is the number of the state. When the number of the extracted ADC bit is $n_{ADC}$, $N = 2^{n_{ADC}}$. Thus, when the number of the extracted ADC bit is $n_{ADC}$, the number of $P(X,Y)$ matrix elements is $N^2$ $(= 2^{n_{ADC}} \times 2^{n_{ADC}})$. In detail, $P(X,Y)$ is the probability density function when an $X$ state is transited to a $Y$ state. The $X$ state and $Y$ state are discrete random variables, which represent a whole set of feasible values during the experiments[44,45]. $X$ is a random variable before the state transition occurs, while $Y$ is also another random variable after the state transition. For example, random variable $X = \{S1, S2, S3, S4\}$ and $Y = \{S1, S2, S3, S4\}$ for $n_{ADC} = 2$. In this case, the number of the state is 4 and the number of the elements in the $P(X,Y)$ matrix is 16 $(= 2^{n_{ADC}} \times 2^{n_{ADC}})$, *i.e.*, the $P(X,Y)$ matrix is represented with $\{P_{(1,1)}, P_{(1,2)}, P_{(1,3)}, \cdots, P_{(4,2)}, P_{(4,3)}, P_{(4,4)}\}$. Figure 5c graphically illustrates the state transition from $X$ to $Y$ and mathematically shows its corresponding matrix form.

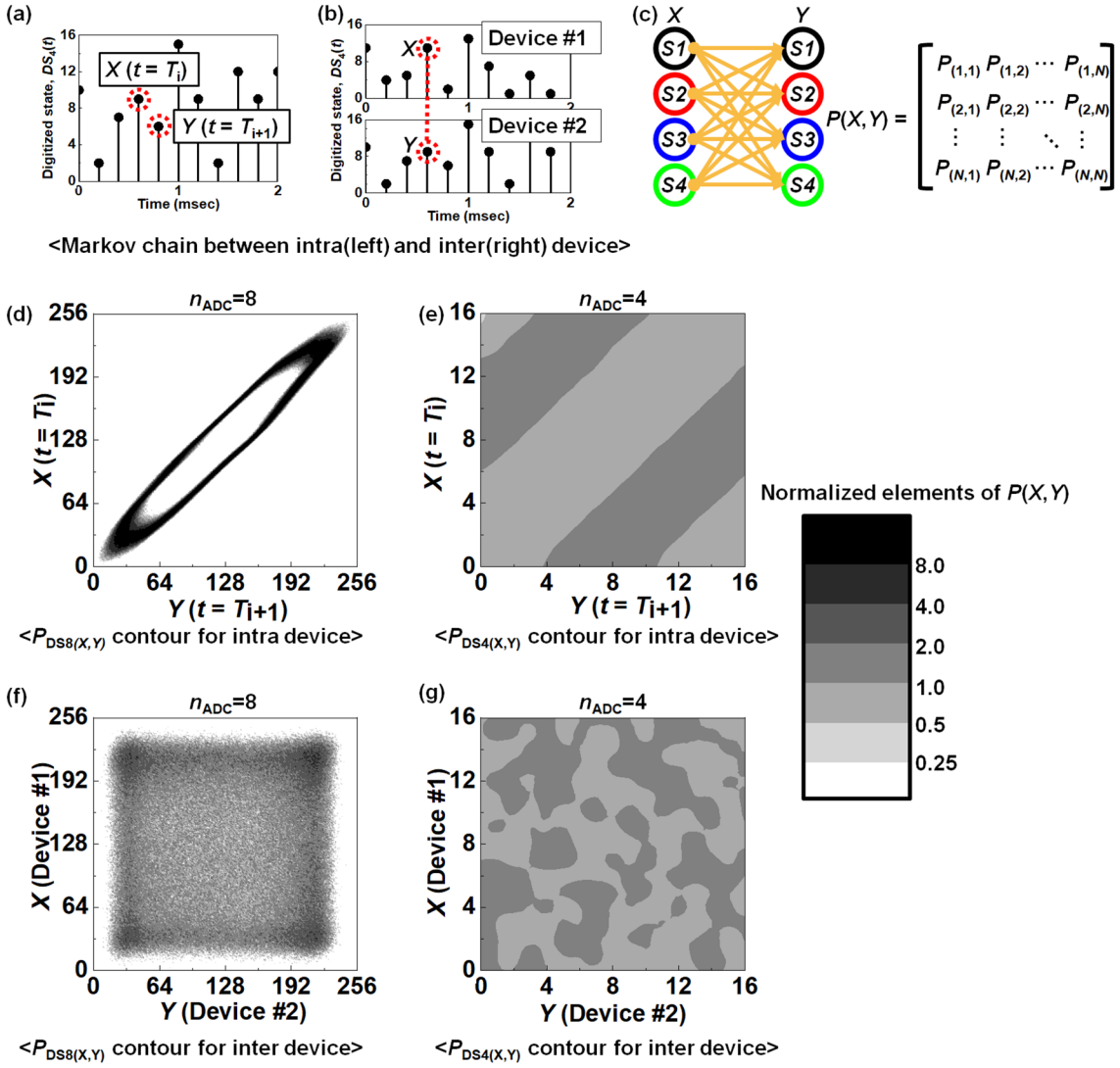


**Figure 5.** Visualization of the Markov chain model between intra and inter devices. (**a**) Schematic illustration to extract $DS_4(t)$ in the Markov chain model for an intra device. (**b**) Schematic illustration to extract $DS_4(t)$ in the Markov chain model between inter devices. The transition probability from $X$ state to $Y$ state is represented by sub-elements in the $P(X,Y)$ matrix. The Markov chain model for an intra device (left) denotes temporal transition according to the time evolution from the $X$ state ($t = T_i$) to $Y$ state ($t = T_{i+1}$), while the Markov chain model between inter devices (right) indicates spatial transition from the $X$ state (device #1) to $Y$ state (device #2). (**c**) Schematic illustration of the state-transition from the $X$ variable to $Y$ variable and its matrix form of $P(X,Y)$. (**d**) Contour map of $P_{DS8(X,Y)}$ for an intra device according to time evolution. (**e**) Contour map of $P_{DS4(X,Y)}$ for an intra device according to time evolution. (**f**) Contour map of $P_{DS8(X,Y)}$ among inter devices. (**g**) Contour map of $P_{DS4(X,Y)}$ among inter devices.

For example, $P_{(4,2)}$ indicates the probability density that state-4 (abbreviated to $S4$) in the random variable $X$ is transited to state-2 (abbreviated to $S2$) in the random variable $Y$. The probability density is normalized so that the total summation of all the $P(X,Y)$ matrix elements is in unity. As another example, the $P(X,Y)$ matrix can have 256 ($=2^4 \times 2^4$) elements for $n_{ADC} = 4$. Therefore, Fig. 5a and b represent the transition of $DS_4(t)$ from random variable $X = \{S1, S2, \cdots, S15, S16\}$ to random variable $Y = \{S1, S2, \cdots, S15, S16\}$.

Figure 5d shows a contour map of the elements from the Markov chain model for an intra device of $DS_8(t)$ and Fig. 5e exhibits that of $DS_4(t)$. The Markov chain model for an intra device computes the state transition according to the time evolution from the $X$-state ($t = T_i$) to the $Y$-state ($t = T_{i+1}$). All the elements were previously normalized and a value of 1 is ideal. This implies perfect uniformity, which is highly desirable for unpredictability. The contour map of Fig. 5d depicts the non-uniform distribution of the digital bits. In non-uniform distribution, a next state is predictable if a current state is revealed. In contrast, the contour map of Fig. 5e shows a uniform distribution of the digital bits ranging from 0.5 to 2 in a greyscale bar. Therefore, a uniform distribution of the digital bits, as in the 4 bits case, is preferred for unpredictability. Figure S6 displays the contour map for $DS_8(t)$, $DS_7(t)$, $DS_6(t)$, $DS_5(t)$, $DS_4(t)$, and $DS_3(t)$. The Markov chain model for an intra device shows that unpredictability is enhanced as the number of bits is reduced.

Figure 5f exhibits the contour map of the Markov chain model for inter devices of $DS_8(t)$, while Fig. 5g shows that of $DS_4(t)$. In terms of RNG operations, it is critically important to generate unpredictable signals for the identical input to different devices[46,47]. The Markov chain model between inter devices computes the state transition between different devices from the $X$-state (device #1) to the $Y$-state (device #2). All the elements were previously normalized and a value of 1 is ideal. The contour map of Fig. 5e exhibits non-uniform distribution where the normalized $P(X,Y)$ at certain regions is larger than 2. As discussed above, if a state of one device is revealed, that of the other devices is predictable for the non-uniform distribution. In contrast, the contour map of Fig. 5g displays uniform distribution and the normalized $P(X,Y)$ is ranges from 0.5 to 2. Consequently, the digital bits from the lower $n_{\mathrm{ADC}}$ are preferred for the unpredictability in the Markov chain model. Figure S7 shows the contour map between the inter devices for $DS_8(t)$, $DS_7(t)$, $DS_6(t)$, $DS_5(t)$, $DS_4(t)$, and $DS_3(t)$.

It is also important to evaluate the unpredictability by a mathematical and statistical method, *e.g.*, joint entropy and mutual information[48–51]. The evaluation of the unpredictability in terms of joint entropy and mutual information is classified into two cases: analyses with an intra device and inter devices, according to the number of extracted bits from the ADC. Thus, four unpredictability metrics are employed by the mathematical and statistical method. Case I is the joint entropy with the intra device, Case II is the joint entropy with inter devices, Case III is mutual information with the intra device, and Case IV is mutual information with inter devices. For a given joint probability distribution $P(X,Y)$ between a random variable $X$ and $Y$, $P(X,Y)$ is a measure of the uncertainty associated with a set of variables by checking $P(X,Y) = P(X)\cdot P(Y)$[52,53]. Probability distributions of $P(X,Y)$, $P(X)$, and $P(Y)$ are represented as follows.

$$P(X,Y) = \begin{bmatrix} P_{(1,1)} & \cdots & P_{(1,N)} \\ \vdots & \ddots & \vdots \\ P_{(N,1)} & \cdots & P_{(N,N)} \end{bmatrix}$$

$$P(X) = \begin{bmatrix} P_1 & \cdots P_j \cdots & P_N \end{bmatrix}, \quad \text{where} P_j = \sum_{l=1}^{N} P_{(j,l)}$$

$$P(Y) = \begin{bmatrix} P_1 & \cdots P_k \cdots & P_N \end{bmatrix}, \quad \text{where} P_k = \sum_{m=1}^{N} P_{(k,m)}$$

The summation for all the components is 1, *i.e.*,

$$\sum_{k=1}^{N}\sum_{j=1}^{N} P_{(j,k)} = 1.$$

$P(X,Y)$ is the joint probability distribution between a random variable $X$ and $Y$. Figure 5d shows the contour map for the intra device when $n_{\mathrm{ADC}} = 8$, Fig. 5e exhibits that for the intra device when $n_{\mathrm{ADC}} = 4$, Fig. 5f displays that for inter devices when $n_{\mathrm{ADC}} = 8$, and Fig. 5g plots that for inter devices when $n_{\mathrm{ADC}} = 4$.

In contrast to the joint probability $P(X,Y)$, $H(X,Y)$ is joint entropy, which is a metric that shows the quantity correlation between random variables $X$ and $Y$[54,55]. The joint entropy is represented with the joint probability distribution, $P(X,Y)$, as follows.

$$H(X,Y) \equiv -\sum_{j=1}^{N}\sum_{k=1}^{N} P_{(j,k)} \cdot \log_2 P_{(j,k)}$$

The joint entropy measures the uncertainty by checking $P(X,Y) = P(X)\cdot P(Y)$, as mentioned above[52,53]. A high level of joint entropy implies that the random variable $Y$ is unpredictable even though the random variable $X$ is unwantedly known. For Case I (joint entropy with the intra device), $H(X(t),Y(t))$ reflects how unpredictable a state transition between different times is. The different times indicate a time lag between $X(t = T_{\mathrm{i}})$ and $Y(t = T_{\mathrm{i+1}})$. For Case II (joint entropy with inter devices), $H(X(t),Y(t))$ represents the spatial correlation strength between random variables $X$ (device #1) and $Y$ (deice #2), *i.e.*, it quantifies a level of the spatial correlation.

Mutual information $I(X,Y)$ is another metric to describe the uncertainty. This is simply calculated by the following.

$$I(X,Y) \equiv H(X) + H(Y) - H(X,Y)$$

$$H(X) = -\sum_{j=1}^{2^n} P_j \cdot \log_2 P_j, \quad \text{where } P_j = \sum_{l=1}^{N} P_{(j,l)}$$

$$H(Y) = -\sum_{k=1}^{2^n} P_k \cdot \log_2 P_k, \quad \text{where } P_k = \sum_{m=1}^{N} P_{(j,m)}$$

Smaller $I(X,Y)$ refers to when the state transition becomes more unpredictable[56,57]. For Case III (mutual information with the intra device), mutual information with temporal variation quantifies a level of time correlation between time intervals by tracing information with past observations at the same position. Therefore, an ideal value of $I(X,Y) = 0$ represents that the observation between infinitely long time intervals cannot influence the unpredictability[58,59]. For Case IV (mutual information with inter devices), mutual information with spatial

variation quantifies a level of device-to-device correlation at the identical time condition. Thus, an ideal value of $I(X,Y) = 0$ denotes that the generated digitized numbers of device #1 are perfectly unpredictable, although the digitized numbers of device #2 are totally revealed.

Figure 6a describes the method to extract joint entropy $H_{intra}(X,Y)$ and mutual information $I_{intra}(X,Y)$ between time intervals at the same device. The $X$ is a variable for a current state ($t = T_i$) and the $Y$ is another variable for a later state ($t = T_{i+1}$). Figure 6b and c exhibit $H_{intra}(X,Y)$ and $I_{intra}(X,Y)$ extracted from a single device, respectively. The $H_{intra}(X,Y)$ shows the unpredictability when $n_{ADC}$ is less than 6. In contrast, $I_{intra}(X,Y)$ shows the unpredictability when $n_{ADC}$ is less than 5. As a result, the unpredictability of the proposed W-RNG is robust to time evolution when $n_{ADC}$ is less than 5, *i.e.*, $n_{ADC} \leq 5$.

On the other hand, Fig. 6d describes a method to extract joint entropy $H_{inter}(X,Y)$ and mutual information $I_{inter}(X,Y)$ between inter devices at the same time. The $X$ is a variable for a state in device #1 and the $Y$ is a variable for another state in device #2. Figure 6e and f plot $H_{inter}(X,Y)$ and $I_{inter}(X,Y)$ extracted from different devices, respectively. These show the device-to-device unpredictability with an identical input condition. The $H_{inter}(X,Y)$ approves that the unpredictability is guaranteed for all $n_{ADC}$. On the contrary, $I_{inter}(X,Y)$ supports that the unpredictability is available when $n_{ADC}$ is less than 5. As a result, the unpredictability of the proposed W-RNG is robust to device-to-device variation when $n_{ADC}$ is less than 5. For visualization, Fig. S8 illustrates the relationship between $H(X,Y)$ and $I(X,Y)$ in Venn diagram form.

Figure 7 shows the unpredictability according to wind velocity ($v_{in}$) introduced to an air gap ($h$) of the W-RNG, and the sampling rate frequency ($f_{SR}$) for $n_{ADC} = 4$. The $H_{intra}(X,Y)$ and $I_{intra}(X,Y)$ are used as a metric to evaluate the unpredictable property for the time evolution. The red dotted lines in Fig. 7 indicate ideal unpredictable signals. Figure 7a and b exhibit $H_{intra}(X,Y)$ and $I_{intra}(X,Y)$ for various $v_{in}$ ranging from 4.2 m/s to 12.8 m/s, respectively. They are also perfectly unpredictable regardless of $v_{in}$. Figure 7c and d display $H_{intra}(X,Y)$ and $I_{intra}(X,Y)$ for various $f_{SR}$ ranging from 10 kHz to 30 MHz. It is well known that the throughput of an RNG linearly increases when an $f_{SR}$ becomes larger. However, Fig. 7c and d show that unpredictability is adversely reduced as the $f_{SR}$ is over 100 kHz. Consequently, unpredictability is sustained as long as the $v_{in}$ is over 4.2 m/s, corresponding to a gentle breeze wind, and the $f_{SR}$ is below 100 kHz.

To evaluate the randomness for each ADC digital output signal, a test suit of the NIST SP 800-22B, which is an authoritative standard to evaluate the randomness of signals generated from an RNG, was used. Figure 8a shows the procedure of making a randomness evaluating report via digital data acquisition. First, digital data of the voltage is generated from the output of 8-pins of the ADC hardware. Next, a randomness test is performed for each ADC digital output signal. Figure 8b represents an average pass rate for the signals of *bit-8* to *bit-1*. This indicates the average value of the pass rate for 15 sub-suites in the NIST SP 800-22B: (1) frequency (mono-bit), (2) frequency within a block, (3) runs, (4) longest run of ones, (5) binary matrix rank, (6) discrete Fourier transform, (7) non-overlapping template matching, (8) overlapping template matching, (9) Maurer's universal statistical, (10) linear complexity, (11) serial, (12) approximate entropy, (13) cumulative sums, (14) random excursions,

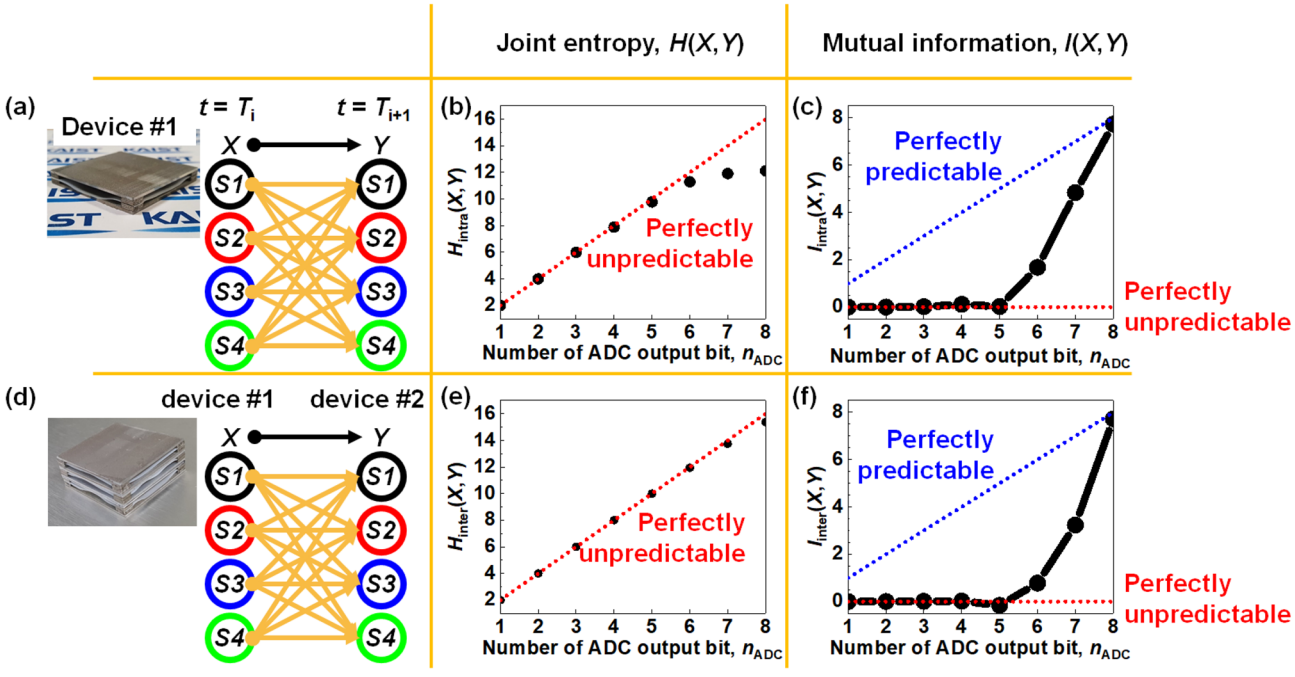


**Figure 6.** Evaluation of unpredictability in terms of joint entropy $H(X,Y)$ and mutual information $I(X,Y)$ for both an intra device and inter devices according to the number of the ADC output bit ($n_{ADC}$). (**a**) Extraction of $H_{intra}(X,Y)$ and $I_{intra}(X,Y)$ in a single device at the same input. (**b**) Extracted $H_{intra}(X,Y)$ between different times. (**c**) Extracted $I_{intra}(X,Y)$ between different times. (**d**) Extraction of $H_{inter}(X,Y)$ and $I_{inter}(X,Y)$ between inter devices at the same time. (**e**) Extracted $H_{inter}(X,Y)$ between device #1 and device #2. (**f**) Extracted $I_{inter}(X,Y)$ between device #1 and device #2.

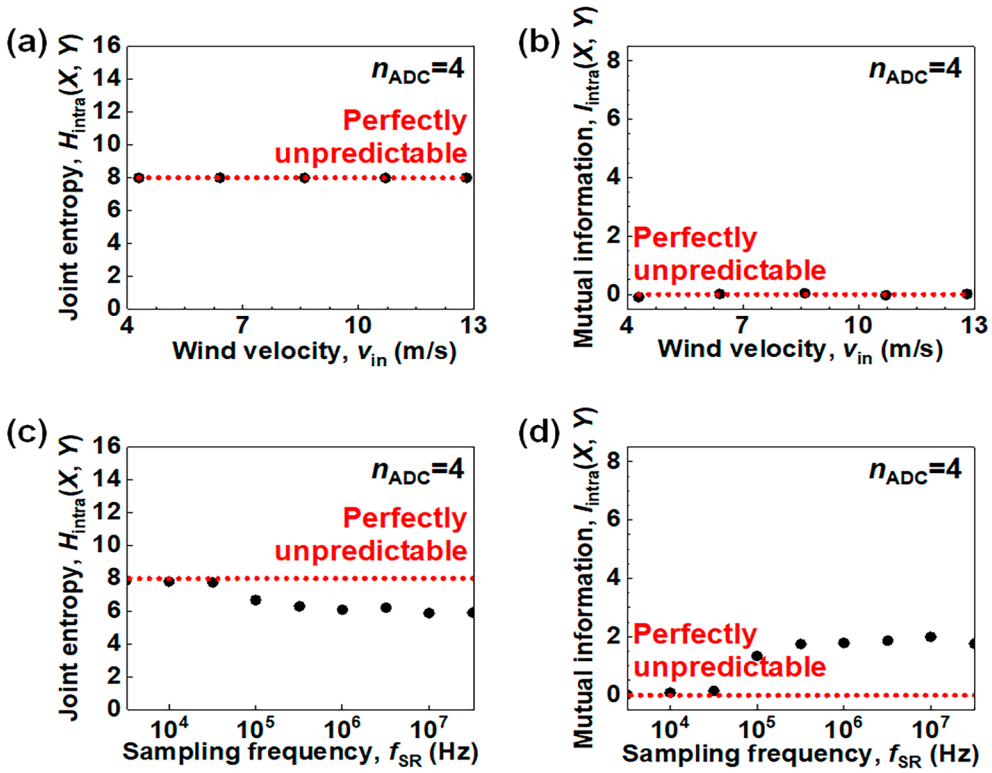


**Figure 7.** Evaluation of unpredictability according to wind velocity ($v_{in}$) and sampling frequency ($f_{SR}$) for an intra device when the number of the ADC output bit ($n_{ADC}$) is 4. (**a**) $H_{intra}(X,Y)$ vs. $v_{in}$. (**b**) $I_{intra}(X,Y)$ vs. $v_{in}$. (**c**) $H_{intra}(X,Y)$ vs. $f_{SR}$. (**d**) $I_{intra}(X,Y)$ vs. $f_{SR}$.

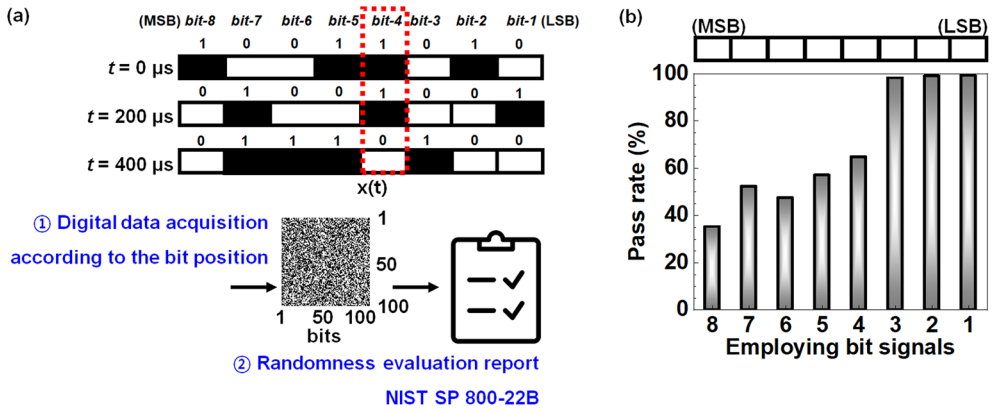


**Figure 8.** (**a**) Schematic of procedure to evaluate the NIST SP 800-22B test according to the ADC digital output signals from *bit-8* (MSB) to *bit-1* (LSB). (**b**) Average pass rate for all sub-suites of NIST SP 800-22B according to the ADC digital output signals from *bit-8* (MSB) to *bit-1* (LSB).

and (15) random excursions variant. These 15 sub-suites are simply classified by four groups according to bit capacities, which are 10 kbits, 1 Mbits, 38,912 bits and 65,536 bits. Sub-suits (1), (2), (3), (4), (11), (12) and (13) tests were conducted 400 times with 10 kbits[60,61]. Sub-suits (7), (8), (9), (10), (14), and (15) tests were conducted 4 times with 1 Mbits. A sub-suit (5) binary matrix rank test was performed 102 times with 38,912 bits. The other sub-suite of (6) discrete Fourier transform was performed 61 times with 65,536 bits. For all the experiments, a significance level ($\alpha$) was set to 0.01. The NIST recommends that $\alpha$ be set to a range between 0.001 and 0.01[61]. If the *p*-value for a sequence test is greater than or equal to $\alpha$, it is considered to have passed the test. In conclusion, digital signals of *bit-3* to *bit-1* possess excellent random properties, whereas those of *bit-8* to *bit-4* are worsened. This data reveals that the random properties are influenced by the bit-*n* ranged from 8 (MSB) to 1 (LSB) and the reduced randomness results in degraded unpredictability.

## Conclusion

This study demonstrated the use of a wind-driven triboelectric nanogenerator, named W-RNG, as a dual-function device that can harvest energy and generate random numbers. The W-RNG has a two-in-one structure. The partial adoption of output digital signals from analog-to-digital converter (ADC) hardware significantly enhanced unpredictable properties, which were analyzed by statistical and mathematical metrics such as auto-correlation, cross-correlation, joint entropy, and mutual information. Auto-correlation and cross-correlation analyses between intra and inter devices reveal that digital signals of *bit-4* to *bit-1* possessed more unpredictability compared with those of *bit-8* to *bit-5*. On the other hand, digital signals showed unpredictable properties in terms of joint entropy and mutual information when the number of ADC bit ($n_{ADC}$) is less than 5. Therefore, the data adoption of *bit-4* among the raw digital bits guaranteed unpredictable properties. These results can pave way to quickly checking whether a used entropy source for a true random number generator (TRNG) is indeed unpredictable in both a theoretical and statistical point of view.

## Data availability

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

Received: 29 April 2023; Accepted: 29 September 2023
Published online: 03 October 2023

## References

1. Vadlamudi, S. & Hargrove, D. L. The Internet of Things (IoT) and social interaction: Influence of source attribution and human specialization. *Eng. Int.* **9**, 17–28 (2021).
2. Choo, K. K. R., Gai, K., Chiaraviglio, L. & Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Comput. Secur.* **102**, 102136 (2021).
3. Wang, J., Lim, M. K., Wang, C. & Tseng, M. L. The evolution of the Internet of Things (IoT) over the past 20 years. *Comput. Ind. Eng.* **155**, 107174 (2021).
4. Manulis, M., Bridges, C. P., Harrison, R., Sekar, V. & Davis, A. Cyber security in new space: Analysis of threats, key enabling technologies and challenges. *Int. J. Inf. Secur.* **20**, 287–311 (2021).
5. Adepu, S., Kandasamy, N. K., Zhou, J. & Mathur, A. Attacks on smart grid: Power supply interruption and malicious power generation. *Int. J. Inf. Secur.* **19**, 189–211 (2020).
6. Melki, R., Noura, H. N. & Chehab, A. Lightweight multi-factor mutual authentication protocol for IoT devices. *Int. J. Inf. Secur.* **19**, 679–694 (2020).
7. Park, J. H. *et al.* A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. *Hum. Centric Comput. Inf. Sci.* **11**, 1–22 (2021).
8. Yaacoub, J. P. A., Noura, H. N., Salman, O. & Chehab, A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *Int. J. Inf. Secur.* **21**, 115–158 (2022).
9. Sangeetha, Y. *et al.* Authentication of symmetric cryptosystem using anti-aging controller-based true random number generator. *Appl. Nanosci.* **1**, 1–10 (2021).
10. Acosta, A. J., Addabbo, T. & Tena-Sánchez, E. Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. *Int. J. Circuit Theory Appl.* **45**, 145–169 (2017).
11. Iavich, M., Kuchukhidze, T., Gnatyuk, S. & Fesenko, A. Novel certification method for quantum random number generators. *Int. J. Comput. Netw. Inf. Secur.* **13**, 28–38 (2021).
12. Lyp, T., Karimian, N. & Tehranipoor, F. LISH: A new random number generator using ECG noises. In *2021 IEEE International Conference on Consumer Electronics,* 1–6 (2021).
13. Seepers, R. M., Strydis, C., Sourdis, I. & Zeeuw, C. I. D. On using a von Neumann extractor in heart-beat-based security. In *2015 IEEE Trustcom/BigDataSE/ISPA,* 491–498 (2015).
14. Yu, A. *et al.* Self-powered random number generator based on coupled triboelectric and electrostatic induction effects at the liquid–dielectric interface. *ACS Nano* **10**, 11434–11441 (2016).
15. Zhu, H., Zhao, C., Zhang, X. & Yang, L. A novel iris and chaos-based random number generator. *Comput. Secur.* **36**, 40–48 (2013).
16. Reezwana, A. *et al.* A quantum random number generator on a nanosatellite in low Earth orbit. *Commun. Phys.* **5**, 314 (2022).
17. Islam, M. S. Using ECG signal as an entropy source for efficient generation of long random bit sequences. *J. King Saud Univ. Comput. Inf. Sci.* **34**, 5144–5155 (2022).
18. Abraham, N., Watanabe, K., Taniguchi, T. & Majumdar, K. A high-quality entropy source using van der Waals heterojunction for true random number generation. *ACS Nano* **16**, 5898–5908 (2022).
19. 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).
20. 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).
21. Park, S. J. *et al.* Self-sustainable wind speed sensor system with omni-directional wind based triboelectric generator. *Nano Energy* **55**, 115–122 (2019).
22. Seol, M. L. *et al.* Vertically stacked thin triboelectric nanogenerator for wind energy harvesting. *Nano Energy* **14**, 201–208 (2015).
23. Rudiyanto, B., Hariono, B. & Budiprasojo, A. quadcopter surveyor drone wind velocity data characteristic for optimal hotwire sensor position. In *Journal of Physics: Conference Series*, vol. 1569 032096 (2020).
24. Massé, C., Gougeon, O., Nguyen, D.-T. & Saussié, D. Modeling and control of a quadcopter flying in a wind field: A comparison between LQR and structured H∞ control techniques. In: *2018 International Conference on Unmanned Aircraft Systems,* 1408–1417 (2018).
25. Liu, S. *et al.* Magnetic switch structured triboelectric nanogenerator for continuous and regular harvesting of wind energy. *Nano Energy* **83**, 105851 (2021).
26. Wang, Z. L., Jiang, T. & Xu, L. Toward the blue energy dream by triboelectric nanogenerator networks. *Nano Energy* **39**, 9–23 (2017).
27. Texas Instruments, ADC08100 Evaluation module user's guide. https://www.ti.com/tool/ADC08100EVM, 2017.
28. Chang, S., AlAshmouny, K., McCormick, M., Chen, Y. C. & Yoon, E. Bio bolt: A minimally-invasive neural interface for wireless epidural recording by intra-skin communication. In *Proc. IEEE Symp. VLSI Circuits,* 146–147 (2011).
29. Yang, Y., Zhou, J., Liu, X., Cheong, J. H. & Goh, W. L. A 151-nW adaptive delta-sampling ADC for ultra-low power sensing applications. *IEEE Trans. Circuits Syst.* **63**, 638–642 (2016).

30. Yip, M. & Chandrakasan, A. P. A resolution-reconfigurable 5-to-10b 0.4-to-1V power scalable SAR ADC. In *Proc. IEEE ISSCC,* 190–192 (2011).
31. 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).
32. Ma, X. *et al.* Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).
33. 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).
34. Carruba, V., Aljbaae, S., Domingos, R. C., Huaman, M. & Barletta, W. Chaos identification through the autocorrelation function indicator. *Celest. Mech. Dyn. Astron.* **133**, 38 (2021).
35. Wu, H., Xu, J., Wang, J. & Long, M. Autoformer: Decomposition transformers with auto-correlation for long-term series forecasting. In *Advances in Neural Information Processing Systems*, vol. 34 (2021).
36. Baltagi, B. H., Song, S. H., Jung, B. C. & Koh, W. Testing for serial correlation, spatial autocorrelation and random effects using panel data. *J. Econom.* **140**, 5–51 (2007).
37. F. Diaz, 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).
38. Lohan, E. S. Statistical analysis of BPSK-like techniques for the acquisition of Galileo signals. *J. Aerosp. Comput. Inf. Commun.* **3**, 234–243 (2006).
39. Zebende, G. F. DCCA cross-correlation coefficient: Quantifying level of cross-correlation. *Phys. A Stat. Mech. Appl.* **390**, 614–618 (2011).
40. Plenkers, K., Ritter, J. R. R. & Schindler, M. Low signal-to-noise event detection based on waveform stacking and cross-correlation: Application to a stimulation experiment. *J. Seismol.* **17**, 27–49 (2013).
41. Kafsi, M., Grossglauser, M. & Thiran, P. The entropy of conditional Markov trajectories. *IEEE Trans. Inf. Theory* **59**, 5577–5583 (2013).
42. Choi, M. C. Velocity formulae between entropy and hitting time for Markov chains. *Stat. Probab. Lett.* **141**, 62–67 (2018).
43. Ricci, L. Asymptotic distribution of sample Shannon entropy in the case of an underlying finite, regular Markov chain. *Phy. Rev. E* **103**, 022215 (2021).
44. Chakraborty, S. Generating discrete analogues of continuous probability distributions—A survey of methods and constructions. *J. Stat. Distrib. Appl.* **2**, 1–30 (2015).
45. Hajar, M., El Badaoui, M., Raad, A. & Bonnardot, F. Discrete random sampling: Theory and practice in machine monitoring. *Mechanical Systems and Signal Processing* **123**, 386–402 (2019).
46. Kim, M., Ha, U., Lee, K. J., Lee, Y. & Yoo, H. J. A 82-nW chaotic map true random number generator based on a sub-ranging SAR ADC. *IEEE J. Solid-State Circuits* **52**, 1953–1965 (2017).
47. Özkaynak, F. Cryptographically secure random number generator with chaotic additional input. *Nonlinear Dyn.* **78**, 2015–2020 (2014).
48. Gong, L., Zhang, J., Sang, L., Liu, H. & Wang, Y. The unpredictability analysis of Boolean chaos. *IEEE Trans. Circuits Syst. II Express Briefs* **67**, 1854–1858 (2019).
49. Inubushi, M. Unpredictability and robustness of chaotic dynamics for physical random number generation. *Chaos Interdiscip. J. Nonlinear Sci.* **29**, 033133 (2019).
50. Karell-Albo, J. A., Legon-Perez, C. M., Madarro-Capo, E. J., Rojas, O. & Sosa-Gomez, G. Measuring independence between statistical randomness tests by mutual information. *Entropy* **22**, 741 (2020).
51. Barigye, S. J. *et al.* Relations frequency hypermatrices in mutual, conditional, and joint entropy-based information indices. *J. Comput. Chem.* **34**, 259–274 (2013).
52. Madiman, M. & Tetali, P. Information inequalities for joint distributions, with interpretations and applications. *IEEE Trans. Inf. Theory* **56**, 2699–2713 (2010).
53. Ma, X., Huang, X., Du, S., Liu, H. & Ning, X. Symbolic joint entropy reveals the coupling of various brain regions. *Phys. A Stat. Mech. Appl.* **490**, 1087–1095 (2018).
54. Chen, L., Singh, V. P. & Guo, S. Measure of correlation between river flows using the copula-entropy method. *J. Hydrol. Eng.* **18**, 1591–1606 (2013).
55. Marco, D. & Neuhoff, D. L. Entropy of highly correlated quantized data. *IEEE Trans. Inf. Theory* **56**, 2455–2478 (2010).
56. Kim, Y. S., Yeom, Y. & Choi, H. B. Online test based on mutual information for true random number generators. *J. Korean Math. Soc.* **50**, 879–897 (2013).
57. Namdari, A. & Li, Z. A review of entropy measures for uncertainty quantification of stochastic processes. *Adv. Mech. Eng.* **11**, 1687814019857350 (2019).
58. Eskafi, M. *et al.* Mutual information analysis of the factors influencing port throughput. *Marit. Bus. Rev.* **6**, 129–146 (2020).
59. Pluim, J. P., Maintz, J. A. & Viergever, M. A. Mutual-information-based registration of medical images: A survey. *IEEE Trans. Med. imaging* **22**, 986–1004 (2003).
60. Sulak, F., Uğuz, M., Kocak, O. & Doğanaksoy, A. On the independence of statistical randomness tests included in the NIST test suite. *Turkish J. Electr. Eng. Comput. Sci.* **25**, 3673–3683 (2017).
61. Georgescu, C. & Simion, E. New results concerning the power of NIST randomness tests. *Proc. Rom. Acad. Ser. A* **18**, 381–388 (2017).


## 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) and the 2018 Open R&D project of the Korea Electric Power Corporation (KEPCO) (R18EO01).

## Author contributions

M.-S.K. and Y.-K.C. wrote the main manuscript text. I.-W.T. prepared Figs. 1, 2, 3. M.-S. K. prepared Figs. 4, 5, 6, 7 and 8. All authors reviewed the manuscript.

## 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/s41598-023-43894-1.

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