Random number generation from a quantum tunneling diode

Kanin Aungskunsiri†, Ratthasart Amarit†, Kruawan Wongpanya, Sakdinan Jantarachote, Wittawat Yamwong, Siriporn Saiburee, Sataporn Chanhorn, Apichart Intarapanich, and Sarun Sumriddetchkajorn

National Electronics and Computer Technology Center,
National Science and Technology Development Agency,
Ministry of Higher Education, Science, Research, and Innovation,
112 Thailand Science Park, Phahonyothin Road, Khlong Nueng, Khlong Luang, Pathum Thani, 12120 THAILAND

(Dated: 31 January 2023, arXiv.2002.02032)

†The author to whom correspondence may be addressed: kanin.aungskunsiri@nectec.or.th.
†These two authors contributed equally to this work.

ABSTRACT

Random numbers are important in many activities, including communication, encryption, science, gambling, finance, and decision-making. There is a strong demand for a hardware random number generator that could support cryptographic applications. In this work, we propose a quantum tunneling diode as a source of true randomness achieved by applying electrical current sweeps through the device and then harnessing a time-counting unit to measure fluctuation of current flows. Our approach can be implemented with inexpensive electronics and could be integrated into systems that require random numbers such as portable communication devices.

Random numbers have many uses in communication, science, mathematics, testing, finance, and gambling. In communication, random numbers are critical for the encryption of sensitive information. The security of communication, in a practical sense, relies on the complexity of an encryption function; achieving that complexity, in turn, demands unpredictability of secret keys. In addition to quantum communication, real-world implementation of quantum-key-distribution protocol demands true randomness in the process of establishing secret keys between trusted nodes—namely, both the sender and the receiver must randomly select quantum states for transmission and detection respectively. In stochastic simulation, random seeds are used in a mechanism to produce parameter values for simulation models with a variety of probability distributions. Randomization is also key in gambling and digital lotteries, especially in casinos, where a dedicated random number generator is vital. In the stock market, randomness is involved in a process of stocks distribution to buyers. Furthermore, verification via online transaction requires unpredictably random seeds for the generation of one-time passwords.

Computer programing generates pseudo-random numbers at a very fast speed in practice, but this source poses a security issue since an output value is calculated from a deterministic process. Electronic noise appears as a random disturbance in an electrical signal. It can serve a useful purpose for random number generation, but this source consists of intrinsic biases given that it is difficult to derive raw random outputs with good statistical properties. Atmospheric noise relates to a chaotic process that involves complexities cooperating with unknown parameters. Though atmospheric noise may be adequate in some applications, it can pose security risks. Namely, since the random signals are not isolated in a closed system, a third party could set up a device to obtain signals coming from the same origin. Exploitations of a quantum property of light in various schemes, such as optical shot noise, phase fluctuation of a laser, vacuum fluctuation, and photon arrival time measurements, are approaches to obtain high bitrate quantum random number generation.

Regarding current technologies mentioned above, entropy sources acquired from the quantum origins are still expensive. Other entropy sources relate to the quantum tunneling effect in various semi-conductor devices such as resonant tunneling diodes, tunnel field-effect transistors, and magnetic tunnel junctions. Among this device category, the tunnel diode as well as its exploitation for high quality random number generation would be of interest.

In this work, we propose an application of a tunnel diode as a key component for obtaining an entropy source. This device operates at room temperature and does not require ex-
A tunnel diode is a solid-state device and one of many types of semiconductor diodes incorporated with a p-n junction. See the supplementary material for a basic introduction of a tunnel diode. The device itself can operate in two modes: (i) a tunneling mode and (ii) a typical p-n junction mode. An ideal plot of current as a function of biased voltage (I-V characteristic) of a tunnel diode is illustrated in Figure 1a. As the figure shows, a tunnel diode has an N-shaped I-V characteristic such that there is a peak current \( I_p \) at a specific bias voltage \( V_p \). This characteristic is due to the collective behavior of tunneling electrons that results in the current flow. In fact, this behavior is different from the case of a single particle described by the quantum mechanics.

Regarding the N-shape of the I-V characteristic, sweeping current \( I \) and measuring voltage \( V \) across a tunnel diode results in a hysteresis cycle. We examined an off-the-shelf tunnel diode (P/N: 3I201D), as shown in Figure 1b, with a circuit diagram, as shown in Figure 1c. An I-V hysteresis loop obtained from our measurements is presented in Figure 1d. Here, \( I_p \) is associated with the value of current where the voltage jumps to the other branch of the hysteresis loop.

Bernardo-Gavito et al. conducted a study of the hysteresis behavior associated with the generation of random numbers, examining the I-V characteristic by performing multiple current sweeps on a resonant-tunneling diode (RTD). In the prior-art, each forward current sweeping through the RTD took a different path along the I-V curve in a random manner. The values of \( I_p \) as measured in their work fluctuated with a random distribution. We adopted this finding and looked for this behavior on a tunnel diode.

We applied a current-source meter to sweep current through a tunnel diode circuit and collected a dataset of I-V values from 450 current sweeps. The extracted values of \( I_p \) are presented in Figure 1e and Figure 1f. Here, we obtained fluctu-
I were converted to the values of current in non-negatively sinusoidal waveform across the tunnel diode. A timer was implemented to obtain the values of the flow diagrams, response time was converted to current. In (a), the voltage source was converted to the current source for sweeping the HDG2022B) was configured to produce non-negatively sinusoidal (a and b) and square (c) voltage with 100 Hz repetition rate. At the end of the flow diagrams, response time was converted to current. In (a), the voltage source was converted to the current source for sweeping the tunnel diode. A timer was implemented to obtain the values of $t_p$, which subsequently were converted to the values of $I_p$. In (b, c), the tunnel diode was removed from the circuit to check if any bias signals were originating from other circuit components apart from the tunnel diode itself.

FIG. 3. Flow diagrams of the experiment. We applied a voltage waveform to the electronic circuit and measured the response time for different scenarios: (a) with a tunnel diode circuit, and (b, c) without a tunnel diode circuit. In the beginning, a waveform generator (model: Hantek HDG2022B) was configured to produce non-negatively sinusoidal (a and b) and square (c) voltage with 100 Hz repetition rate. At the end of the flow diagrams, response time was converted to current. In (a), the voltage source was converted to the current source for sweeping the tunnel diode. A timer was implemented to obtain the values of $t_p$, which subsequently were converted to the values of $I_p$. In (b, c), the tunnel diode was removed from the circuit to check if any bias signals were originating from other circuit components apart from the tunnel diode itself.

FIG. 4. Current time series obtained from (a) a complete circuit having a tunnel diode circuit, (b) a voltage comparator circuit, and (c) a voltage signal generator, according to circuit diagrams (a)–(c) in Figure 3, respectively.
voltage signal generator by implementing the circuit diagram as depicted in Figure 3c. Data were collected from 5,000 current sweeps for each test. The results are presented in Figure 4.

Figure 4 presents experimental data on the amplitude fluctuation of the current signals measured from three different tests. We calculated the standard deviations (σ) of the datasets and realized that σ_a > σ_b > σ_c. Even though we detected noise from other parts of the circuit, the noise is very limited and could be negligible. The noise might be coming from errors of the experiment; we leave this potential issue for further investigation.

![Counts](image)

**FIG. 5.** Histogram showing values of $I_p$ obtained from the tunnel-diode circuit (red solid line) in comparison with a Gaussian model plot (dashed line) featuring the standard deviation of 7.7 µA. The dataset is collected from 100,000 current sweeps.

By following the flow diagram in Figure 3a, we collected an additional dataset from 100,000 current sweeps and obtained the statistical distribution shown in Figure 5. We incorporated this result that suggests a Gaussian model for determining a suitable amplitude used for the current sweeping. The amplitude which is not too large allows us to obtain signals with good resolution. Accordingly, we managed to collect 20,000 samples per second.

In the implementation, raw signals were collected from the values of $I_{tp}$. An offset is removed from the raw signals for digitization; consequently, binary outputs, as raw data, were extracted from the entropy source. Next, we followed the NIST SP800-90B and implemented a software provided by the NIST to assess the entropy source. This toolkit consists of two main steps: (i) determining the evaluation track, IID (independent and identically distributed) or non-IID, and (ii) estimating the minimum entropy rate of the raw data depending on the determined track. If the raw data fall into an IID track, entropy is considered from the most common value (MCV) estimation. Otherwise, entropy is assessed from the lowest value of entropy estimated from 10 estimators, which are (1) MCV estimation, (2) collision estimation, (3) Markov estimation, (4) compression estimation, (5) t-Tuple estimation, (6) longest repeated substring (LRS) estimation, (7) multi most common in window prediction (multiMCW) estimation, (8) lag prediction estimation, (9) multiMMC Prediction estimation, and (10) LZ78Y prediction estimation.

According to the NIST SP800-90B, our raw data are determined as non-IID. Table I shows the results of min-entropy evaluated from 10 estimators. Five datasets of 40 million-bit sequences were examined. Here, the compression estimation provides the lowest value of min-entropy, given that the assessed min-entropy, $H_{\infty}$, was 0.62 on average. This value reflects the lower bound of random bits we can achieve from the raw data. As shown in Table I, the raw data have stable entropy.

These raw data were not ready for real-world use, and they did not pass the NIST SP800-22 examination for statistical randomness. Post processing was mandatory to improve the raw data quality. We implemented Toeplitz-hashing extractor with the raw data to render uniformly distributed random outputs. This extractor employs a binary matrix with a dimension of $m \times n$, where $m$ and $n$ correspond to the output and input bit-string length, respectively. $m$ is considered from the value of assessed min-entropy such that $m \leq nH_{\infty}$. Security parameter is a measure of the statistical distance between the distribution of the dataset and the ideal uniform distribution. By implementing the Toeplitz extractor, the security parameter of the post-processed data is estimated from $2^{(m-nH_{\infty})/2}$.

In the implementation, we set $n = 4096$. Hence, $m \leq 2539$. We chose $m = 2296$. Thus the Toeplitz matrix has a size of $2296 \times 4096$, providing that the security parameter is below $2^{100}$.

The post-processed data, as the final outputs, were rechecked with the NIST SP800-90B. The outputs at this stage passed the IID test. Therefore, the min-entropy was determined from the MCV estimation. Table II shows min-entropy assessed from the raw data and the final outputs. The result shows improvement of the statistical properties, and almost full entropy is achieved.

To validate the statistical randomness of the final outputs, a hundred datasets of 1,000,000-bit sequences were examined with 15 sub-methods in accordance to the NIST SP800-22 Test Suite Compliance. The test results, as presented in Table III, indicate that the final outputs passed the NIST SP800-22 with a significance level of 0.01.

We also used the same dataset to check for the presence of repeating pattern and evaluate the degree of similarity by performing autocorrelation analysis. As plotted in Figure 6, the result indicates no sign of periodic pattern over 100 successive bit intervals. Therefore, the final outputs have no repeating pattern over an acceptable range.

To conclude, we investigated the I-V characteristic of a tunnel diode and examined the behavior of its hysteresis cycle. Forward current sweeping takes a slightly different path in each cycle. This random variation is associated with the measured values of $I_p$, and it can serve as an entropy source. We demonstrated a utilization of a time-counting module to measure the values of $t_p$ that are associated with events in which voltages jump to the other branch of the hysteresis loop. As a result, a random distribution was obtained. We demonstrated this proposed technique with inexpensive electronics. Our preliminary prototype used a computer to assess...
TABLE I. Entropy assessment of raw data according to the NIST SP800-90B. Each dataset contains 40 million-bit sequences. The values of assessed min-entropy were selected from the lowest values from 10 estimators.

| Estimator      | Dataset 1 | Dataset 2 | Dataset 3 | Dataset 4 | Dataset 5 |
|----------------|-----------|-----------|-----------|-----------|-----------|
| MCV            | 0.999 313 | 0.999 373 | 0.999 259 | 0.999 325 | 0.999 403 |
| Collision      | 1.000 000 | 1.000 000 | 1.000 000 | 1.000 000 | 1.000 000 |
| Markov         | 0.901 064 | 0.899 539 | 0.899 158 | 0.898 290 | 0.895 731 |
| Compression    | 0.619 087 | 0.622 348 | 0.623 679 | 0.624 235 | 0.625 367 |
| t-Tuple        | 0.872 663 | 0.867 644 | 0.874 429 | 0.881 406 | 0.872 663 |
| LRS            | 0.895 813 | 0.914 673 | 0.852 600 | 0.881 406 | 0.865 663 |
| MultiMCW       | 1.000 000 | 1.000 000 | 1.000 000 | 1.000 000 | 1.000 000 |
| Lag Prediction | 0.977 310 | 0.878 794 | 0.964 168 | 0.975 876 | 0.976 249 |
| MultiMMC Prediction | 0.853 159 | 0.857 779 | 0.857 333 | 0.855 688 | 0.855 221 |
| LZ78Y Prediction | 0.899 739 | 0.897 203 | 0.897 819 | 0.896 944 | 0.894 367 |

Assessed min-entropy: 0.619 087

TABLE II. Entropy assessment of raw data versus final outputs according to the NIST SP800-90B. Final outputs in each dataset were extracted from 40 million-bit sequences of raw data.

| Assessed min-entropy | Dataset 1 | Dataset 2 | Dataset 3 | Dataset 4 | Dataset 5 |
|----------------------|-----------|-----------|-----------|-----------|-----------|
| Raw data             | 0.619 087 | 0.622 348 | 0.623 679 | 0.624 235 | 0.625 367 |
| Final outputs        | 0.998 865 | 0.998 956 | 0.998 919 | 0.998 804 | 0.999 194 |

TABLE III. NIST SP800-22 test results of 100 million-bit sequences collected from the final outputs. To pass this test suite at a significance level of 0.01, two conditions are required for each of the 15 sub-methods: (i) the P-values-total must be higher than $10^{-4}$, and (ii) the proportion must be higher than 96/100.

| Method                  | P-values-total | Proportion | Result |
|-------------------------|----------------|------------|--------|
| Frequency               | 0.224 821      | 100/100    | Pass   |
| Block Frequency         | 0.779 188      | 99/100     | Pass   |
| Runs                    | 0.096 578      | 99/100     | Pass   |
| Longest Run             | 0.304 126      | 100/100    | Pass   |
| Rank                    | 0.574 903      | 99/100     | Pass   |
| Fast Fourier Transform  | 0.366 918      | 98/100     | Pass   |
| Overlapping Template    | 0.003 201      | 99/100     | Pass   |
| Universal               | 0.911 413      | 100/100    | Pass   |
| Linear Complexity       | 0.015 598      | 100/100    | Pass   |
| Approximate Entropy     | 0.455 937      | 99/100     | Pass   |
| Non-overlapping Template| 0.514 124      | 100/100    | Pass   |
| Serial                  | 0.249 284      | 99/100     | Pass   |
| Cumulative Sums         | 0.181 557      | 100/100    | Pass   |
| Random Excursions       | 0.062 821      | 99/100     | Pass   |
| Random Excursions Variant| 0.008 266     | 99/100     | Pass   |

Autocorrelation calculated from a dataset of 100 million-bit sequences collected from the final outputs.
that is also heavily doped, but Zener diode is incomparable to the tunnel diode as the former has a relatively lower doping concentration.

FIG. S1. Energy level of a p-n semiconductor. The band gap between the conduction band \((E_c)\) and the valence band \((E_v)\) of a typical p-n junction diode is wide and behaves like a thick barrier. This barrier blocks the passage of electrons flowing across the p-n junction. Electrons with energy greater than the barrier can overcome the internal potential force and cause a current flow.

In the case of a typical p-n junction diode, the n-type conduction band aligns at the p-type bandgap (Figure S1). In this scenario, the depletion region behaves like a potential barrier that blocks the passage of electrons flowing from p-type to n-type. The current can flow only when the electrons have energy that surpasses the obstructive force as illustrated in Figure S2a.

In contrast, a tunnel diode in which electrons can pass through a narrow barrier is depicted in Figure S2b. The device itself can operate in two modes: (i) tunneling mode and (ii) typical p-n junction mode as shown in Figure S3. It can be explained as follows. At a stage where bias voltage drops to zero (Figure S3a), the conduction band of the n-type sits below the valence band of the p-type. By applying small bias (Figure S3b), electrons can tunnel through the depletion region, resulting in the current flow from the conduction band of the n-side to the valence band of the p-side. In this scenario, the rise of the bias voltage increases the probability of electrons flowing, corresponding to the tunneling effect, until the conduction band of the n-side and the valence band of the p-side become fully overlapped (Figure S3c). As a result, there is a peak current \((I_p)\) at a specific bias voltage \((V_p)\). Increasing the voltage level causes these bands to begin to separate (Figure S3d), and the chance of electron tunneling declines until the bands are fully out of alignment at a certain voltage \((V_c)\) (Figure S3e). At \(V_c\), the tunneling effect diminishes and therefore provides no contribution to the current flow \((I_c)\). During \(V_p\) to \(V_c\), where current and biased voltage translate in the opposite direction, negative resistance behavior is exhibited. Applying more voltage will drive the tunnel diode to operate in a typical p-n junction state where current and biased voltage translate in the same direction.

REFERENCES AND NOTES

1 Random numbers are employed for the estimation for the value of pi in the Buffon’s needle problem. See http://www.cut-the-knot.org/fta/Buffon/buffon9.shtml (Accessed 1 May 2021).
2 C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of IEEE International Conference on Computers, Systems and Signal Processing 17, 8 (1984).
3 A. K. Ekert, “Quantum cryptography based on bell’s theorem,” Physical Review Letters 67, 661–663 (1991).
4 P. D. Townsend, “Secure key distribution system based on quantum cryptography,” Electronics Letters 30, 809–811 (1994).
5 H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Physical Review Letters 94, 230504 (2005).
6 Y. Zhao, B. Qi, and H.-K. Lo, “Experimental quantum key distribution with active phase randomization,” Applied Physics Letters 90, 044106 (2007).
7 P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O’Brien, “Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client,” Physical Review Letters 112, 130501 (2014).
8 D. Crnjac Milič and L. Kvesić, “Role of random numbers in simulations of economic processes,” Interdisciplinary management research 4, 562–570 (2008).
Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers (Walter de Gruyter GmbH & Co KG, 2018).

P. L’Ecuyer, “Software for uniform random number generation: Distinquishing the good and the bad,” in Proceeding of the 2001 Winter Simulation Conference (Cat. No. 01CH37304), Vol. 1 (IEEE, 2001) pp. 95–105.

J. T. Gleeson, “Truly random number generator based on turbulent electro-convection,” Applied Physics Letters 81, 1949–1951 (2002).

A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, “Fast physical random bit generation with chaotic semiconductor lasers,” Nature Photonics 2, 728–732 (2008).

I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, “Fast physical random bit generation with chaotic semiconductor lasers,” Nature Photonics 2, 728–732 (2008).

L. Esaki, “New phenomenon in narrow germanium p-n diode tunneling through a single diode,” Scientific Reports 7, 1949–1951 (2017).

J. Qin, X. Wang, C. Qu, C. Wai, L. Huang, C. Guo, T. Yu, H. Wei, and X. Han, “Thermally activated magnetization back-hopping based true random number generator in nano-ring magnetic tunnel junctions,” Applied Physics Letters 114, 112401 (2019).

D. Vodenicarevic, N. Locatelli, A. Mizrahi, J. S. Friedman, A. F. Vincent, M. Romera, A. Fukushima, Y. Yukihi, H. Kubota, S. Yuasa, S. Tiwari, J. Grollier, and D. Querlioz, “Low-energy truly random number generator with superparamagnetic tunnel junctions for unconventional computing,” Physical Review Applied 8, 054045 (2017).

A. Stefanov, G. v. Battum, I. Verbauwhede, M. Wakker, and B. Yang, “Design and testification,” in Proceeding of the 2018 IEEE 23rd European Test Symposium (ETS) (2018) pp. 1–10.

B. Astbury, J. Roberts, J. Sexton, B. Ashbury, J. Balasch, F. Bernard, V. Fischer, M. Grujić, M. Laban, O. Petura, V. Rožić, G. v. Battum, I. Verbauwhede, M. Wakker, and B. Yang, “Design and testing methodologies for true random number generators towards industry certification,” in 2018 IEEE 23rd European Test Symposium (ETS) (2018) pp. 1–10.