Hardware Comparison Of Analog Entropy Sources For True Random Number Generation Using Zener Diodes, MEMS Sensors, And Audio Noise

Lutfi Hamdan
Independent Researcher, Texas, USA
ORCID: 0009-0003-8117-4263
lutfinazam4@gmail.com

***Abstract*—This manuscript presents a comprehensive experimental and analytical comparison of three low-cost physical entropy sources suitable for hardware true random number generators (TRNGs): an amplified electret microphone (MAX9814), avalanche noise from a reverse-biased Zener diode, and micro-vibration signals obtained from a MEMS accelerometer (ADXL345). A Raspberry Pi Pico microcontroller was employed for uniform acquisition, and extensive statistical and NIST SP 800-90B–inspired evaluations were conducted. The results demonstrate that microphone noise provides the highest raw variance but exhibits correlation, Zener avalanche noise yields stable high-quality entropy, and accelerometer-based entropy is comparatively weak unless combined with post-processing or mixing.**

Keywords—component True Random Number Generator; Entropy Source; Zener Diode Noise; MEMS Accelerometer; Embedded Security; NIST SP 800-90B.

1. Introduction

True random number generators rely on unpredictable physical phenomena rather than deterministic algorithms. Applications include cryptographic key generation, secure boot mechanisms, hardware security modules, and physically unclonable systems. While avalanche diodes are widely used in commercial TRNGs, modern low-cost embedded platforms integrate sensors whose intrinsic noise properties may also provide entropy.

This paper evaluates three such sources under identical acquisition and processing conditions, quantifying their entropy characteristics and assessing their suitability for hybrid TRNG architectures.

2. Hardware Architecture

A Raspberry Pi Pico microcontroller served as the data acquisition platform. Its 12-bit ADC sampled analog sources, while the ADXL345 accelerometer communicated via I2C. Data were streamed to a host PC over USB serial.

2.1. Microphone Interface.

The MAX9814 module provided an amplified signal biased around mid-supply.

2.2. Zener Diode Interface.

A 6.7 V Zener diode was reverse biased through a 1 kΩ resistor from a regulated supply. The noise component was AC-coupled, biased at mid-supply, amplified using a TL072 operational amplifier, and attenuated to remain within the ADC range.

2.3. Accelerometer Interface.

The ADXL345 sensor was configured for ±2 g operation. Differential extraction between successive samples isolated stochastic components from static gravitational offsets.

3. Mathematical Modeling

We model each sampled signal as a discrete time sequence:

$$x[n] = \mu + \eta[n].$$

The term μ denotes the DC bias at the ADC input. The term η[n] denotes the stochastic noise component.

We compute the sample mean as:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i.$$

We compute the sample standard deviation as:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2}.$$

These quantities describe signal centering and spread.

3.

3.1. Binary Extraction

We convert analog samples into bits by thresholding about the mean:

$$b[n] = \begin{cases} 1, & x[n] > \mu, \\ 0, & x[n] \leq \mu. \end{cases}$$

For accelerometer data, we remove slow drift by differencing:

$$d[n] = x[n] - x[n-1].$$

We apply the same threshold rule to d[n] with μ=0

3.2 Zener Diode Noise Model

A reverse biased Zener diode generates avalanche current noise.
Shot noise power density follows:

$$S_I = 2qI.$$

The symbol q denotes the electron charge. The symbol I denotes the diode current.

The front-end amplifier scales this noise before digitization.

3.3 Temporal Dependence

We evaluate correlation between adjacent samples using lag one autocorrelation:

$$R(1) = \frac{1}{N\sigma^2} \sum_{n=1}^{N-1} (x[n] - \mu)\,(x[n+1]$$

Large values indicate memory in the sequence. Small values indicate near independent samples.

3.3 Entropy Estimation

We estimate min entropy using:

$$H_{\min} = -\log_2 (p_{\max})\,.$$

The pmax denotes the probability of the most frequent symbol.

This metric bounds extractable randomness per sample.

4. Data Processing and Metrics

For each configuration, 100,000 samples were recorded. Histograms and time-series plots assessed distributional properties. Bitstreams were derived by thresholding at the mean (or zero for differential signals). Bias, transition rates, and lag-1 autocorrelation were computed.

Entropy estimates followed NIST SP 800-90B concepts, including most-common-value–based min-entropy.

5. Results

The microphone exhibited the largest variance, followed by Zener avalanche noise and accelerometer-derived signals. While microphone entropy was high, silence conditions introduced significant correlation, motivating whitening. Zener-based entropy was comparatively stable. Accelerometer entropy was weak and unsuitable as a standalone source.

Figure sets illustrate representative histograms, time-domain behavior, and logarithmic-scale variance comparison.

6. NIST SP 800-90B–Style Evaluation

Min-entropy, bias, and lag-1 correlation were computed for all sources. Table 1 summarizes the results. Zener avalanche noise achieved consistently high min-entropy with low correlation, while accelerometer-derived entropy was poor unless mixed with other sources. Microphone signals showed strong entropy but temporal correlation in quiet environments, indicating the necessity of post-processing.

7. Discussion

The comparison highlights practical design trade-offs between amplitude, stability, and environmental sensitivity. Zener-based sources are attractive for compact TRNG designs, while microphones require shielding and decorrelation. Accelerometers are best used as auxiliary sources in multi-source mixers. Hybrid architectures employing XOR folding or cryptographic hashing across heterogeneous sources are recommended.

8. Conclusion

Three low-cost entropy mechanisms were evaluated under a unified experimental framework. Zener avalanche noise emerged as the most robust single-source candidate, microphone noise delivered strong but correlated entropy, and MEMS accelerometer signals were weakest. The methodology and results support future work on hybrid embedded TRNG architectures compliant with modern statistical standards.

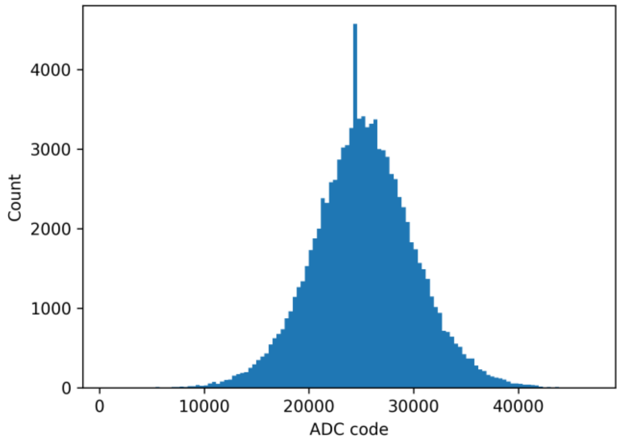

***Figure 1.** Histogram of microphone ADC samples recorded under ambient noise conditions using 100,000 samples.*

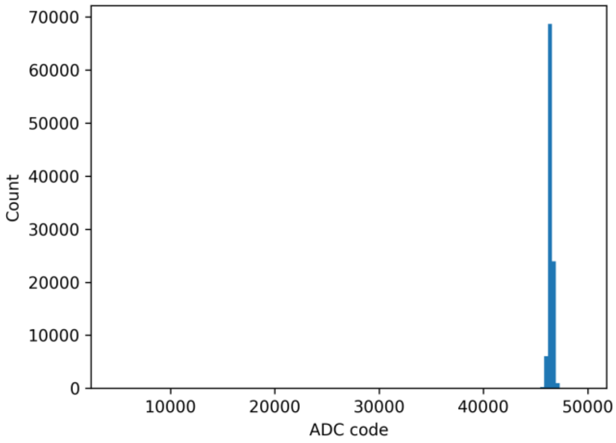

***Figure 2.** Histogram of amplified Zener diode ADC samples showing the raw distribution at the digitizer input.*

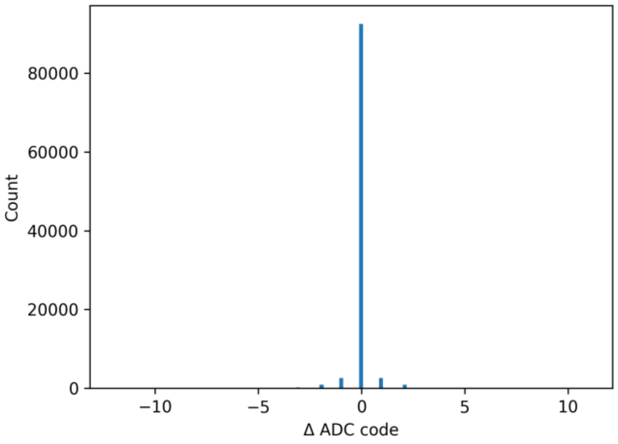

***Figure 3.** Histogram of ADXL345 differenced samples that removes slow drift and highlights high frequency motion noise.*

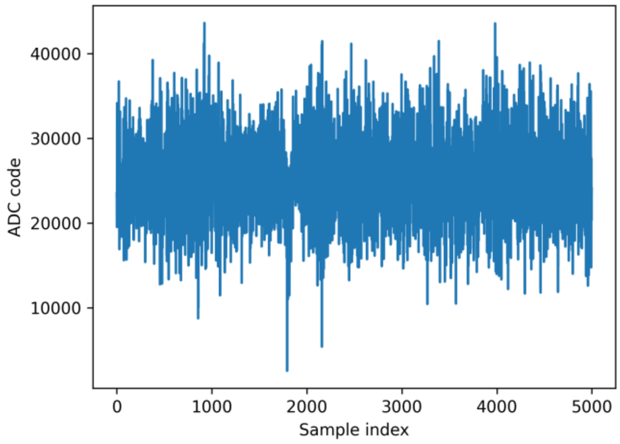

***Figure 4.** Time series of microphone ADC samples for the first 5000 acquisitions.*

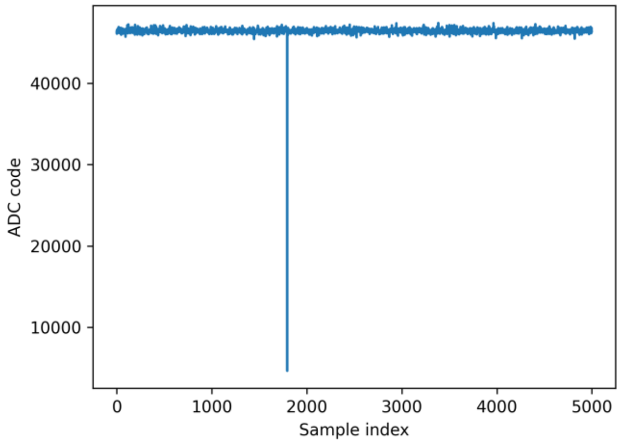

***Figure 5.** Time series of amplified Zener diode ADC samples for the first 5000 acquisitions.*

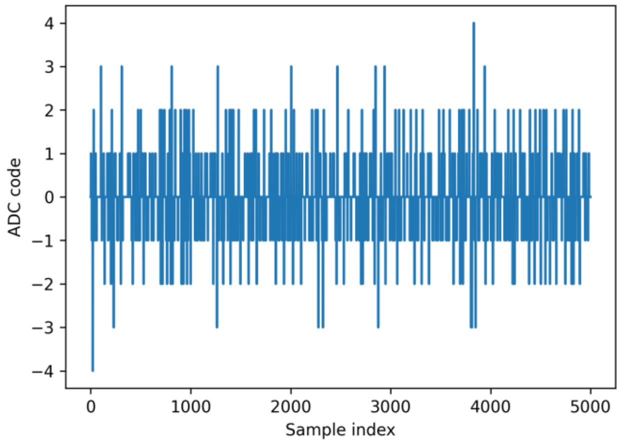

***Figure 6.** Time series of ADXL345 differenced samples for the first 5000 acquisitions.*

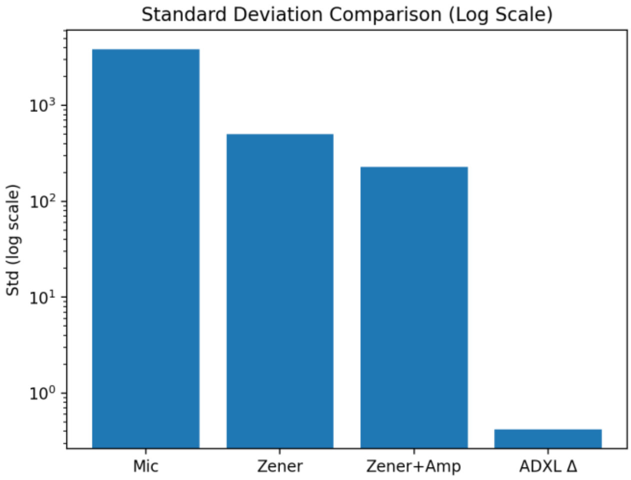

***Figure 7.** Standard deviation of raw ADC codes for the three entropy sources.*

***Table 1**. Statistical summary of the raw ADC samples for the three entropy sources.*

Source	Min-Entropy (bits/sample)	Bias	Lag-1 Corr
Mic (silence)	0.9739	0.0091	0.8003
Mic (noise)	0.9743	0.0090	-0.0662
Zener + Amp	0.9537	0.0163	0.0668
ADXL Δ	0.0542	0.4631	-0.0000

NIST SP 800-22 Subset Checks

We ran a small NIST SP 800-22 subset on the bitstreams. We report p-values for the Frequency test, Runs test, and Approximate Entropy test with m = 2. We show results after Von Neumann debiasing. We also show results after a SHA-256 conditioner that hashes 2048 input bits into 256 output bits.

Source	VN bits	SHA bits	VN p(Freq)	VN p(Runs)	VN p(AE m=2)	SHA p(Freq)	SHA p(Runs)	SHA p(AE m=2)
Mic (noise)	25026	3072	0.2016	0.1363	0.0394	0.5637	0.2981	0.7899
Zener (am-pli-fied)	25089	3072	0.7379	0.4007	0.7847	0.9712	0.1123	0.1866
Zener (raw)	25596	3072	0.9203	0.8026	0.7524	0.5883	0.8610	0.8714
ADXL (delta)	5526	512	0.2585	0.0000	0.0000	0.9296	0.7239	0.9076

***Table 2.** NIST SP 800-22 subset test results with Von Neumann debiasing and SHA-256 conditioning.*

The raw sources show bias and correlation at the sample level. Debiasing removes the main bias but it does not remove all dependence. The SHA-256 conditioner produces blocks that pass this subset for the tested sources.

Patents

No patents result from the work reported in this manuscript.

Supplementary Materials:

Supplementary materials are available with this manuscript.
Figure S1: Extended histograms for all entropy sources.
Table S1: Full statistical metrics for each dataset.

***Author Contributions:** Conceptualization, L.H.; methodology, L.H.; software, L.H.; validation, L.H.; formal analysis, L.H.; investigation, L.H.; resources, L.H.; data curation, L.H.; writing—original draft preparation, L.H.; writing—review and editing, L.H.; visualization, L.H.; supervision, L.H.; project administration, L.H.*

Funding:

This research received no external funding. The APC was not funded by any agency.

***Data Availability Statement:** The datasets generated and analyzed during this study are available from the corresponding author upon reasonable request.*

***Acknowledgments:** During the preparation of this manuscript, the author used ChatGPT (GPT-5.2, OpenAI) for language editing and formatting assistance. The author reviewed and edited the output and takes full responsibility for the content of this publication.*

***Conflicts of Interest:** The author declares no conflicts of interest.*
The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. *Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. Handbook of Applied Cryptography; CRC Press: Boca Raton, FL, USA, 1996.*
2. *Rukhin, A.; Soto, J.; Nechvatal, J.; et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications; NIST SP 800-22 Rev. 1a; NIST: Gaithersburg, MD, USA, 2010.*
3. *Turan, M.S.; Barker, E.; Kelsey, J.; et al. Recommendation for the Entropy Sources Used for Random Bit Generation; NIST SP 800-90B; NIST: Gaithersburg, MD, USA, 2018.*

4. *Von Neumann, J. Various techniques used in connection with random digits. Appl. Math. Ser.* ***1951****, 12, 36–38.*

5. *Petrie, C.S.; Connelly, J.A. A noise-based IC random number generator for applications in cryptography. IEEE Trans. Circuits Syst. I* ***2000****, 47, 615–621.*

6. *Suciu, A.; Varga, B.; Iantovics, L. True random number generators based on semiconductor noise. Microelectron. J.* ***2014****, 45, 591–599.*

7. *Analog Devices. ADXL345 Data Sheet. Available online: https://www.analog.com (accessed on 25 January 2026).*

Disclaimer/Publisher's Note: *The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of JMEST and/or the editor(s). JMEST and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.*