

Thermal Stress Effects on Physical Entropy in Quantum and True Random Number Generators

M. Inga, L. G. M. Riveros, J. B. Rosolem, E. Mobilon, A. C. Paixão, L. R. Pizzini, T. Sutili, and R. C. Figueiredo
CPQD – Telecom R&D Center
Campinas, São Paulo, Brazil

Abstract—This work examines how thermal stress (0 °C to 60 °C) affects the physical entropy of commercial Quantum (QRNG) and True (TRNG) Random Number Generators. Using the NIST SP 800-90B test suite, we show that elevated and extreme temperatures induce hardware-level structural asymmetries. With the macroscopic chi-square test, we find that TRNG deteriorate approximately linearly with temperature, while QRNG displays more complex but effectively temperature-invariant behavior due to active hardware compensation. We further show that fixed-rate cryptographic extractors can mask these physical degradations, silently weakening information-theoretic security. These findings highlight the need for adaptive and environment-sensitive randomness extraction to ensure robust cryptographic security under realistic operating conditions.

Keywords—Quantum random number generators, True random number generators, Cryptographic randomness extraction, Thermal stress, Information-theoretic security, NIST SP 800-90B, Min-Entropy, Chi-Square Test.

I. INTRODUCTION

The emergence of the second quantum revolution represents a fundamental paradigm shift in contemporary technology, moving beyond passive observation of quantum phenomena toward deliberate engineering, manipulation, and control of individual quantum states. This transition provides the basis for the development of transformative quantum technologies in computing, precision metrology, and secure communication systems. In the domain of cryptography, for example, the security of information is based on the generation of cryptographic keys composed of intrinsically unpredictable sequences of random bits, a process that requires reliable and physically grounded sources of randomness [1].

Traditionally, classical TRNGs extract randomness from complex and chaotic classical processes (thermal noise, oscillator jitter, or chaotic dynamics) governed by classical physics [2, 3]. Although these processes are effectively unpredictable in practice, classical mechanics is, in principle, fully deterministic. Consequently, given arbitrarily large computational resources and sufficiently precise knowledge of the relevant initial conditions and system dynamics, the raw output of a classical TRNG could, at least in theory, be predicted. QRNGs circumvent this limitation by exploiting the intrinsic

indeterminism of quantum measurement outcomes, thereby furnishing a source of entropy that is, under appropriate assumptions, secure in an information-theoretic sense. [4, 5].

Despite this physical distinction, the post-processed output quality of well-designed TRNGs and QRNGs is effectively indistinguishable: both successfully pass standard statistical test suites for randomness (e.g., NIST SP 800-22 and Dieharder). The essential difference lies in their operational paradigms with respect to the roles of signal and noise. In a TRNG, classical noise—such as thermal noise or avalanche noise—constitutes the target signal and, therefore, must be carefully isolated from extraneous external perturbations. By contrast, in a QRNG, the desired signal is a genuinely quantum process. As a result, any classical contribution, including thermal fluctuations in the detection apparatus, functions as a contaminant that diminishes the extractable quantum entropy. This dichotomy leads to a key physical hypothesis: TRNGs and QRNGs should exhibit fundamentally different responses to thermal stress, because the increased temperature serves as an enhanced source of usable signal for the former, while it operates as a direct source of decohering contamination for the latter.

In practice, mitigating this form of contamination is challenging because both QRNGs and TRNGs depend on physical hardware, such as optical modules, photodetectors, and analog-to-digital converters (ADCs), that is intrinsically susceptible to environmental fluctuations. Thermal stress can introduce systematic physical biases, for example, by increasing dark count rates in quantum sensors or inducing threshold drifts in classical diodes. Critically, it is harder to detect these hardware-level biases by analyzing the post-processed output of the device. Modern random number generators typically employ cryptographic extractors (e.g., SHA-256 or AES) to compress and sanitize non-ideal raw data, thereby transforming strongly biased input sequences into outputs that appear statistically uniform.

This masking effect induces a misleading perception of security. The actual information-theoretic entropy supplied to the extractor can decrease substantially under thermal stress without activating any diagnostic mechanisms or alerts. If the extraction rate is not dynamically adjusted to compensate for this physical induced entropy degradation, the generated cryptographic keys will exhibit intrinsically reduced entropy, thereby rendering the system theoretically susceptible.

To address this critical security vulnerability, the present work aims to empirically characterize the influence of temperature variations on the entropy quality of commercial TRNG

This project was supported by the Brazilian Ministry of Science, Technology and Innovation, with resources from Law No. 8,248 of October 23, 1991, under the PPI SOFTEX program, coordinated by Softex and published under PDI 06 (protocol No. 01245.002635/2023-36) in the Brazilian Federal Official Gazette.

The authors can be contacted via the email: marvyn@cpqd.com.br.

and QRNG devices. By systematically evaluating raw output streams under controlled thermal stress conditions, this study seeks to quantify the extent to which temperature perturbs the underlying physical entropy sources and to assess whether these state-of-the-art generators can reliably preserve their cryptographic resilience in realistic operational environments.

II. METHODOLOGY

In this study, we comparatively evaluated a quantum-based random number generator (QRNG; CryptaLabs Firefly) and a classical thermodynamic random number generator (TRNG; TetroLabs SwiftRNG). Despite their different physical origins, both devices implement an analogous three-stage processing pipeline for the generation of cryptographically secure keys. The pipeline begins at the physical entropy source, i.e., the hardware layer in which intrinsically non-deterministic phenomena are harnessed. According to the manufacturers technical specifications, SwiftRNG derives entropy from electrical noise produced by two independent reliable sources, each based on avalanche breakdown in Zener diodes. In contrast, Firefly employs a Quantum Optics Module (QOM) as its primary entropy source.

Subsequently, during the digitization stage, the physical analog signal is sampled and converted into a binary sequence. Due to the intrinsic imperfections of any physical measurement process, the resulting raw data cannot be perfectly random and unavoidably exhibit statistical biases and correlations. These physical non-idealities are empirically observable in Fig. 1(a), where the raw data histograms for Firefly QRNG display non-uniform byte distributions.

Although the detailed architecture of the Firefly remains proprietary, its raw data distribution provides informative evidence on its underlying physical behavior. The histogram indicates an overwhelming dominance of zero-valued bytes, whereas the remaining non-zero bytes approximate a Gaussian distribution that is consistent with the expected quantum noise characteristics. This pronounced over-representation of zeros is a well-documented engineering artifact in unconditioned optical sensing systems [4, 5].

It is also important to recognize that certain devices expose an intermediate output prior to the application of cryptographic post-processing. For example, Fig. 1(b) presents the Firefly's raw noise output, which corresponds to a lightly conditioned sequence obtained after preliminary debiasing associated with

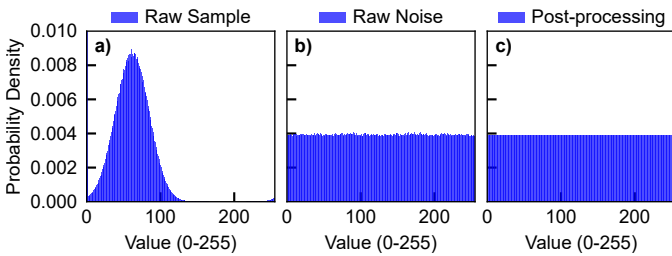


Fig. 1. Probability density distributions of the CryptaLabs Firefly QRNG output states at room temperature: (a) unconditioned raw sample exhibiting digitizer baseline bias, (b) lightly conditioned raw noise intermediate component, and (c) fully post-processed uniform output.

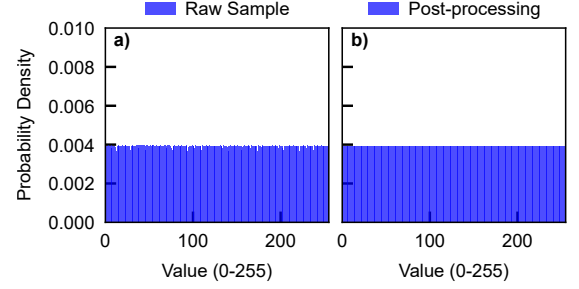


Fig. 2. Probability density distributions of the TetroLabs SwiftRNG TRNG output states at room temperature: (a) unconditioned flat raw sample and (b) fully post-processed uniform output.

built-in health tests. In contrast, the SwiftRNG raw data histogram, illustrated in Fig. 2(a), appears nearly uniform even at this early stage, with no evident requirement for analogous light conditioning. This discrepancy suggests either that the SwiftRNG entropy source inherently produces a more uniform physical distribution at the output of the analog-to-digital converter compared to the biased baseline observed in the quantum module or that the device internally performs an undisclosed preliminary debiasing operation directly on its nominally raw output.

Ultimately, because neither raw nor lightly conditioned data can be reliably employed directly in security-critical applications, such data must be subjected to rigorous cryptographic post-processing. In this final stage, the bit sequence is provided as input to a randomness extractor, typically implemented by a cryptographic hash function such as SHA-256. This algorithm maps a long, potentially biased bit stream to a shorter sequence, that is, to an excellent approximation, statistically uniform and consisting of independent bits. The effectiveness of this extraction step is empirically corroborated in Fig. 1(c) and Fig. 2(b), where the histograms of the post-processed data exhibit essentially flat, unbiased distributions.

To characterize the quality of the entropy sources and to assess the influence of thermal stress on unconditioned or minimally conditioned data, the following main quantitative metrics were evaluated.

A. Min-Entropy

Min-entropy characterizes the worst-case scenario by quantifying the difficulty an adversary faces in correctly predicting the most probable output of an entropy source. This metric is used to evaluate the unpredictability of the unconditioned hardware. Formally, the min-entropy (H_∞) of a discrete random variable or byte output (X) is defined as the negative binary logarithm of the maximum probability within its distribution:

$$H_\infty(X) = -\log_2 \left(\max_{x \in \mathcal{X}} \Pr(X = x) \right) \quad (1)$$

where $\mathcal{X}$ is the domain of possible values (0 to 255). To quantify this metric, we adopted the non-IID (non-Independent and Identically Distributed) assessment track specified in NIST SP 800-90B [6]. This protocol employs a dual-track framework to estimate entropy from two complementary structural perspectives: the symbol-level min-entropy (H_{original}) and the

bit-string-level min-entropy ($H_{\text{bitstring}}$). The quantity H_{original} characterizes the predictability of multi-bit symbols (specifically, 8-bit words), thereby capturing macroscopic distributional biases, whereas $H_{\text{bitstring}}$ evaluates the data at the level of individual bits to identify microscopic temporal correlations and latent sequential dependencies. To obtain a conservative lower bound on the physical randomness of the source, the standard prescribes the selection of the minimum of the two estimates, according to

$$H_{\text{final}} = \min(H_{\text{original}}, 8 \times H_{\text{bitstring}}),$$

which is applicable for samples with 8-bit resolution.

At room temperature, applying this formulation to the raw Firefly output, shown in Fig. 1(a), we obtain a very low minimum entropy (< 1 bits/byte), which is mainly driven by the overwhelming predominance of zero-valued bytes. However, as discussed previously, this does not necessarily indicate a malfunction or fundamental limitation of the underlying quantum physical source; rather, it is largely attributable to baseline-dominated digitization artifacts.

By contrast, the raw output of the SwiftRNG device, depicted in Fig. 2(a), exhibits a substantially higher minimum entropy of 7.47 bits/byte, consistent with a considerably more uniform baseline distribution of the digitized data. Notably, an almost identical minimum entropy of 7.47 bits/byte is obtained for the lightly conditioned Firefly output (see Fig. 1(b) for the corresponding non-vetted conditioning stage).

For fully post-processed output sequences generated by both devices, shown in Fig. 1(c) and Fig. 2(b), the estimated min-entropy reaches the theoretical upper bound of 8 bits/byte. This saturation indicates that min-entropy is not a suitable diagnostic metric for assessing fully hashed sequences, since the cryptographic extraction process effectively obscures any residual structure or correlations originating from the underlying physical source.

B. The Chi-Square Goodness-of-Fit Test

To evaluate the statistical uniformity of the output data, we use the chi-square (χ^2) goodness-of-fit test, which measures how far the empirical distribution of generated values deviates from an ideal uniform distribution. For a truly uniform random sequence, each byte value should occur with equal probability. The chi-square statistic is

$$\chi^2 = \sum_{i=0}^{k-1} \frac{(O_i - E)^2}{E}, \quad (2)$$

Here, k is the number of possible outcomes ($k = 256$ for byte values 0–255), O_i is the observed frequency of the i -th byte value, and E is the expected frequency under uniformity, given by $E = N/k$, where N is the total number of samples.

A higher value of χ^2 indicates a stronger deviation from the theoretically expected uniform distribution, thus revealing the presence of structural biases in the bit stream. Consequently, this metric is particularly appropriate for assessing the lightly conditioned output of the Firefly device as well as the raw output of the SwiftRNG. Because the underlying hypothesis test assumes an ideal perfectly uniform distribution, the statistic χ^2

provides a highly sensitive indicator of even subtle deviations from this reference model.

III. EXPERIMENTAL SETUP

To investigate the influence of thermal stress on entropy sources, we employed a Superohm CC200TD/010 climatic chamber. This apparatus provided a precisely regulated and temporally stable temperature environment, effectively isolated from external perturbations.

The devices under test were exposed to a temperature sweep from 0 °C to 60 °C in discrete increments of 10 °C. At each temperature setpoint, a stabilization period was established before the start of data acquisition. This waiting period was methodologically essential to ensure that the internal components of the random number generators (RNGs) had attained thermal equilibrium with the chamber environment. In terms of hardware integration, the devices utilized distinct communication busses consistent with their architectural specifications: the Firefly module was interfaced via a Peripheral Component Interconnect (PCI) bus, whereas the SwiftRNG device was connected through a standard USB interface.

For each temperature condition, datasets of size 1.2 GB were collected using Linux command-line utilities supplied by the manufacturer. Given the comparatively high nominal bit-generation rates of the devices—20 Mbit/s for the Firefly and 29 Mbit/s for the SwiftRNG—the corresponding acquisition intervals were necessarily short, remaining below 8 min and 6 min, respectively. These short capture intervals confer an experimental advantage by substantially reducing the risk of transient thermal fluctuations influencing the data during collection.

Subsequent to acquisition, the datasets were subjected to a comprehensive suite of statistical tests to characterize the effect of thermal stress on the underlying physical entropy, including the procedures outlined in NIST SP 800-90B and additional batteries such as ENT and Dieharder. In the analysis that follows, we restrict attention to the specific metrics defined in the preceding section.

IV. RESULTS

The initial statistical analysis concentrates on the raw data generated by the Firefly QRNG over the temperature range 0 °C to 60 °C. Fig. 3 displays the min-entropy estimators (H_{original} , $8 \times H_{\text{bitstring}}$, and H_{final}) computed using the NIST SP 800-90B non-IID analysis protocol. For each temperature, the analysis compares the subsets 1 MB and 10 MB extracted from the entire 1.2 GB data set. A larger sample size of 10 MB is used here to obtain a more accurate and statistically representative estimate of the entropy. This approach increases the robustness of the assessment by reducing the likelihood of statistical underestimation.

As shown in Fig. 3, the estimated min-entropy of the Firefly raw data remains consistently low (approximately 0.97 bits/byte), largely independent of both temperature and sample size. As discussed in the methodology, this reduced value is primarily due to the high fraction of zero-valued bytes in the output distribution. Although Fig. 3 suggests a

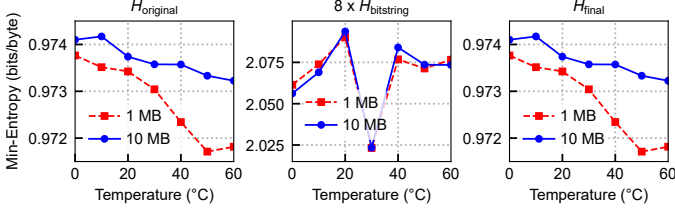


Fig. 3. NIST SP 800-90B min-entropy estimators (H_{original} , $8 \times H_{\text{bitstring}}$, and H_{final}) for the Firefly QRNG unconditioned raw sample across the thermal spectrum (0 °C to 60 °C), comparing the standard 1 MB track against the extended 10 MB analysis window.

slight decrease in min-entropy with increasing temperature, examination of the axis scaling reveals that this variation is restricted to the third decimal place and is therefore attributable to algorithmic noise or other negligible fluctuations. Consequently, the Firefly raw data demonstrate that the min-entropy metric, considered in isolation, can be misleading when evaluating environmental effects on biased quantum digitizers.

Because the Firefly raw data are strongly dominated by baseline digitization artifacts, they exhibit an exceptionally low min-entropy estimate. As a result, the intermediate, lightly conditioned output stream constitutes a more reliable diagnostic probe for characterizing the underlying physical quantum source. To accurately assess the intrinsic environmental robustness of both devices, we applied the NIST SP 800-90B statistical test suite to the lightly conditioned Firefly data and to the raw SwiftRNG data, analyzing the 1 MB and 10 MB subsets drawn from the entire 1.2 GB datasets. The evaluation focuses on three quantities as functions of temperature: H_{original} , $8 \times H_{\text{bitstring}}$ and H_{final} .

Inspection of Fig. 4 and Fig. 5 indicates that the conventional sample size 1 MB induces pronounced statistical instability in the estimates for both devices. Within these smaller subsets, the NIST estimators disproportionately penalize short-term statistical fluctuations, leading to spurious collapses in the bit-string min-entropy. This, in turn, drives the final min-entropy estimate downward, producing a highly erratic and misleading representation of the hardware response over the thermal range. When the analysis window increases to 10 MB, these systematic underestimations are largely suppressed, resulting in a more stable baseline and exposing the true structural performance limits of the digitizers.

As illustrated in Fig. 5, a temperature-dependent physical susceptibility is observed for SwiftRNG when using

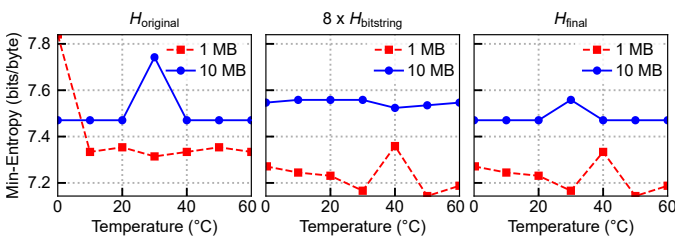


Fig. 4. NIST SP 800-90B min-entropy estimators (H_{original} , $8 \times H_{\text{bitstring}}$, and H_{final}) for the Firefly QRNG lightly conditioned raw noise as a function of temperature, highlighting the stabilization provided by the 10 MB dataset.

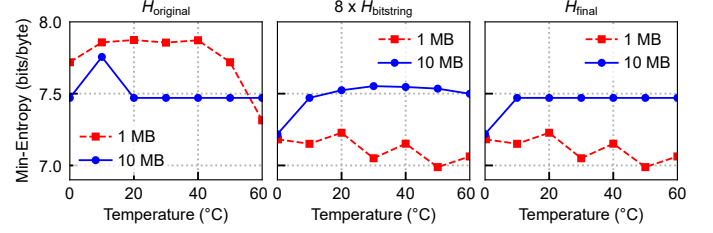


Fig. 5. NIST SP 800-90B min-entropy estimators (H_{original} , $8 \times H_{\text{bitstring}}$, and H_{final}) for the TetroLabs SwiftRNG TRNG unconditioned raw sample as a function of temperature, exposing the microscopic thermal correlation drop at 0 °C.

the subsets 10 MB as a stable reference, which produce an approximately constant value of 7.47 bits/byte under nominal operating conditions. At the lower thermal boundary of 0 °C, the scaled bit-string min-entropy ($8 \times H_{\text{bitstring}}$) exhibits a marked decrease, dropping below the symbol-level min-entropy threshold (H_{original}). As a result, the ultimately validated min-entropy is stringently limited by this increased bit-level predictability and undergoes a substantial degradation.

This characteristic response indicates that exposure to extreme cold induces microscopic temporal correlations in the analog output of the Zener-diode based noise source. By contrast, the lightly conditioned final min-entropy of the Firefly remains effectively invariant throughout the investigated temperature range, demonstrating a pronounced robustness at the microscopic bit level.

According to Firefly specifications, environmental perturbations influence internal optical components and thereby trigger QRNG AutoCalibration procedures. These routines dynamically adapt hardware control parameters in real time to compensate for thermally induced variations. Consequently, the observed stability of entropy in the lightly conditioned output can be primarily attributed to this active AutoCalibration mechanism, which suppresses physical bias in the raw quantum signal.

Although statistical assessment based on 10 MB NIST is well suited to detect such microscopic temporal vulnerabilities, the min-entropy metric is intrinsically sensitive to the predictability of the worst case and does not directly characterize the macroscopic distributional symmetry of the noise process. Therefore, to obtain a comprehensive characterization of the structural degradation of the sources of physical entropy over the full thermal range, it is necessary to complement the min-entropy with an additional global distribution metric, such as the chi-squared statistic χ^2 .

For this purpose, an asymptotic chi-square (χ^2) analysis was conducted on complete 1.2 GB datasets obtained from both Firefly (lightly conditioned raw noise) and SwiftRNG (unprocessed raw samples), using the ENT Linux utility. Since the χ^2 statistic scales linearly with the sample size (N), processing the entire file acts as a macroscopic statistical amplifier. This methodology effectively discriminates persistent thermodynamic biases from short-term stochastic fluctuations, thereby providing a highly sensitive measure of the extent to which prolonged thermal stress perturbs the global physical symmetry of the generated entropy.

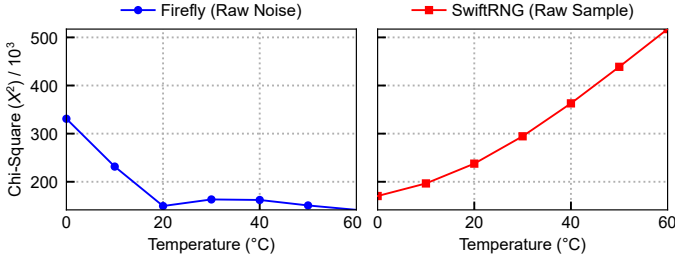


Fig. 6. Asymptotic Chi-Square (χ^2) goodness-of-fit distribution as a function of operating temperature for the Firefly QRNG (lightly conditioned raw noise sample) and SwiftRNG TRNG (unconditioned raw sample) evaluated over the comprehensive 1.2 GB datasets.

As illustrated in Fig. 6, the two devices exhibit markedly different thermodynamic susceptibilities. For SwiftRNG, the parameter χ^2 increases approximately linearly with temperature, increasing from about 170×10^3 in 0°C to more than 517×10^3 in 60°C . This behavior indicates a pronounced, monotonic degradation of the Zener-diode-based analog entropy source at elevated temperatures, whereby enhanced thermal noise substantially distorts the macroscopic output distribution. In contrast, the Firefly displays an opposite temperature dependence. Its value χ^2 attains a pronounced maximum under freezing conditions (0°C), reaching approximately 330×10^3 , and subsequently stabilizes at a substantially lower level (between 140×10^3 and 160×10^3) at higher temperatures. This pattern suggests that the underlying quantum entropy source, most likely governed by the dark-count statistics of the photon detector, is structurally more vulnerable to extreme cold than to elevated temperatures.

Ultimately, these macroscopic fluctuations provide evidence that extreme environmental conditions substantially modify the underlying analog physical processes governing both TRNG and QRNG architectures. Because these pronounced physical asymmetries circumvent statically calibrated on-chip hardware conditioning mechanisms (e.g., simple XOR operations or least significant bit extraction), the global statistical uniformity of the output bit-stream is intrinsically compromised. This observation reveals a fundamental hardware constraint: static combinational logic cannot adapt to slow or non-stationary environmental drifts, thereby necessitating the deployment of dynamic, cryptographically secure extractors—such as SHA-256—to ensure robust and provable resilience.

V. CONCLUSION

Empirical evaluation of both raw and minimally post-processed outputs across a range of generation temperatures is crucial for ensuring the cryptographic robustness of commercial random number generators deployed in operational environments. As shown, hardware-level constraints—such as the baseline bias that saturates the Firefly’s raw bitstream with zeros—can artificially obscure the underlying thermodynamic instabilities and temporarily improve the apparent cryptographic unpredictability. Under these conditions, lightly conditioned outputs offer an especially informative diagnostic regime. Because this intermediate representation is produced by simple, statically calibrated debiasing procedures intended

primarily for online health monitoring, it remains sufficiently transparent to reveal large-scale physical asymmetries that conventional raw min-entropy analyzes may fail to detect.

Although cryptographically post-processed data can exhibit statistical uniformity, macroscopic degradation quantified through statistics χ^2 has critical implications for information-theoretic security. If the underlying analog entropy source—whether a quantum photodetector or a classical Zener diode—degrades under thermal stress and produces reduced physical entropy per byte, the cryptographic extractor must, in principle, consume a larger volume of raw data to distill a genuinely secure 256-bit key.

In practice, however, commercial devices typically employ a fixed hard-coded extraction ratio at the firmware level, often calibrated for near-optimal performance under nominal conditions (e.g. 30°C). When extreme environmental stress modifies the physics of the analog device, the entropy rate decreases, yet the device continues to emit keys that successfully pass standard statistical randomness test suites. However, these keys contain substantially less physical entropy than intended. Such a silent degradation of the entropy content structurally weakens the key material, thus increasing its predictability and reducing the effective search space. Consequently, the fundamental physical (or quantum) security margin of the keys is compromised, creating opportunities for sophisticated prediction strategies or significantly more feasible brute-force attacks.

Finally, although conventional statistical metrics applied to post-processed data typically fail to capture these environmentally induced vulnerabilities, alternative analytical frameworks may still be capable of resolving underlying thermodynamic signatures, even following extensive cryptographic extraction. Future work should investigate more sophisticated topological and sequential descriptors, such as random-walk-based analyzes [7], to develop more rigorous assessment methodologies to quantify and compare the thermal robustness of fully conditioned quantum and classical entropy sources.

REFERENCES

- [1] E. Mobilon, J. B. Rosolem, M. Inga, L. G.M. Riveros, T. Suttili, A. C.P. Paixão, A. M. Braga, and R. C. Figueiredo. From classical to quantum-safe security: The transformative role of quantum technologies. *2025 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference, IMOC 2025*, pages 363–371, 2025.
- [2] Vittorio Bagini and Marco Bucci. A design of reliable true random number generator for cryptographic applications. In *International workshop on cryptographic hardware and embedded systems*, pages 204–218. Springer, 1999.
- [3] Fei Yu, Lixiang Li, Qiang Tang, Shuo Cai, Yun Song, and Quan Xu. A survey on true random number generators based on chaos. *Discrete Dynamics in Nature and Society*, 2019(1):2545123, 2019.
- [4] M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89:015004, 2 2017.
- [5] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2:16021–, 6 2016.
- [6] M. A Sönmez Turan, E. Barker, J. Kelsey, K. McKay, Mary L Baish, and Mike Boyle. Nist special publication 800-90b recommendation for the entropy sources used for random bit generation. 2018.
- [7] L. G.M. Riveros, M. Inga, J. B. Rosolem, E. Mobilon, T. Suttili, and R. C. Figueiredo. Evaluating quantum randomness: Random-walk-based characterization of quantum-random number generators. *2025 SBFoton International Optics and Photonics Conference, SBFoton IOPC 2025*, 2025.