



Structural and Electrical Variability of Functional Materials for Cryptographic Key Generation in Quantum-Resistant Hardware

Siva Lingam Thejavath¹, Aktham Adi²

¹Project Manager, High Voltage Cables, Riyadh Cables Company, Riyadh, Saudi Arabia. Email: tejavathshiva@gmail.com. ORCID: 0009-0005-6165-2584

²Department of Physics, Faculty of Science, Al-Nahrain University, Baghdad, Iraq. Email: aktham.oday.sci25@nahrainuniv.edu.iq

Received:- 29/05/2026, Revised:- 26/07/2026, Accepted:- 10/09/2026, Published:- 26/09/2026

ABSTRACT

Security into quantum-resistant hardware needs to be built more than just cryptographic algorithms and must take advantage physically hard to duplicate properties. This work was aimed at investigating the potential for using the structure and electric properties of functional materials for hardware-based generation of cryptographic keys. The structural properties were grain size, film thickness, surface roughness, defect density, porosity, crystallinity, lattice parameter and phase purity, and the electrical properties were conductivity, resistance, dielectric constant, leakage current, switching voltage and impedance. These properties were converted into hardware fingerprints of the devices and tested with uniqueness, reproducibility, bit balance, Hamming distance, entropy, stable-key rate and bit-error rate. The results revealed significant structural and electrical device variations in functional materials with high cryptographic performance. The uniqueness of the Mean PUF approached 50%, the maximum inter-device Hamming distance was greater than 97%, and the Shannon entropy was almost 1 bit per bit. Uniqueness, reproducibility and entropy were positively correlated with structural variability, while key bit-error rate was negatively correlated with both structural and electrical variability. The entropy, uniqueness, reproducibility and stable-key performance reported by devices that met the hardware-readiness requirements was far more robust than that of non-ready devices. The findings suggest that the functional-material variability could be a valuable physical entropy source and hardware root of trust for cryptographic key generation. The method can be used for non-quantum cryptographic designs to enhance secure embedded hardware against cloning, key derivation, and device authentication.

Keywords: functional materials; cryptographic key generation; physical unclonable functions; hardware security; post-quantum cryptography

1. Introduction

The speedy development of quantum computing has raised important worries for the security of traditional cryptographic systems in the long run. Today, public-key approaches are employed in authentication, key exchange and for digital signatures, and as quantum computational power increases these may be at risk and an alternative cryptographic approach that is secure in the post-quantum setting is needed (Mattsson et al., 2021). This shift isn't just for software algorithms; secure digital systems rely on hardware platforms, embedded devices, communication modules and physical security mechanisms as well. As a result, there is a need for coordinated improvements in the cryptographic algorithms, hardware architectures, and physical sources of randomness that can be used to establish secure keys and authenticate devices (Bishwas & Sen, 2024). Quantum related vulnerabilities are relevant to long-lived, connected equipment and critical operational technologies in industrial and cyber-physical systems and could lead to compromised cryptographic infrastructure (Vermeer et al., 2024).

Hardware security has thus emerged as an important factor in the design of post-quantum security. Security properties can be provided by physical unclonable functions, true random number generators, side-channel-resistant circuits, and hardware roots of trust which are difficult to reproduce by software alone (Chowdhury et al., 2020). Process variation, physical randomness, and physical behaviour are now viewed as assets for creating unique authentication responses and material for cryptography (Srinivas & Elango, 2024). Resilient authentication has also been shown to be possible using advanced physical systems that rely upon complex hardware responses that cannot be repeated outside the physical system (He et al., 2024). These methods offer an effective starting point to consider how to use differences arising from the functionality of the materials to create security features specific to the device (Alutaibi, 2025).

Functional materials from a materials-engineering point of view are inherently variable in terms of microstructure, composition, morphology, defects, grain boundaries, thickness, crystallinity and electrical transport behaviour. These variations can affect conductivity, resistance, impedance, dielectric response, leakage current and switching characteristics. However, these differences should not only be manufacturing variations, but they can also be used as physical entropy sources to generate hardware fingerprints and cryptographic keys. The benefits of hardware derived characteristics for robustising secure communication and authentication mechanisms are already illustrated by the hardware-based key establishment approaches (Bhatia et al., 2025). Likewise, it has been found that unconventional material and biological assemblies can be explored as sources of complex physical responses for cryptographic applications, highlighting the emerging activity of material-dependent security primitives (Moukogiannis et al., 2025). Combining randomness provided by the hardware with post-quantum algorithms also offers a viable way to create more robust cryptographic architectures (Zhang et al., 2025).

Post-quantum security is also being pondered at the system level in the context of IoT devices, distributed networks, authentication infrastructures and next generation communication systems. Lightweight and robust security is needed in connected-device environments as the resources may be limited, and larger, more complex cryptographic mechanisms (computation-intensive) cannot be implemented (Gharavi et al., 2024). Lattice-based algorithms have become a prominent contender for post-quantum security, but they still need to be carefully considered for implementation complexity and hardware requirements (Nguyen et al., 2025). This is also the case in post-quantum public-key infrastructures and certificate systems, where secure authentication needs to be guaranteed in the face of heterogeneous devices and networks (Yusof et al., 2025). In addition, hybrid architectures of authentication and key-agreement are being studied for future communication systems to leverage existing schemes and add post-quantum protection (Turnip et al., 2025).

However, little work has focused on the direct link between the variability of functional materials, their electrical response, and their cryptographic key-generation performance. Previous work has focussed on either cryptographic algorithms, communication protocols or system-level implementation and the variability at the material level is not often considered as an integrated security resource. The shift from traditional security systems to quantum resistant security architectures also demonstrates the importance of additional layers of physical security to supply entropy and device uniqueness (Nieto-Morales et al., 2025). The deployment of new PQ schemes in hardware-heavy infrastructures also reveals that besides the choice of the algorithm, implementation constraints must be considered for PQ security (Carroll et al., 2024). Hence, determining structural and electrical variability to hardware derived cryptographic keys could afford an interdisciplinary route to link materials engineering to quantum resistant secure hardware.

Objectives

- To characterize the structural and electrical variability of functional materials relevant to hardware-based security applications.
- To evaluate the relationships between material characteristics and cryptographic performance indicators, including entropy, uniqueness, reproducibility, and key stability.
- To assess the potential of material-derived electrical fingerprints for cryptographic key generation in quantum-resistant hardware systems.

2. Materials and Methods

2.1 Study Design

A quantitative computational study was carried out to determine the correlation between structural and electrical variability of functional materials and their use in cryptographic key generation for quantum resistant hardware. The structural, electrical and security-related parameters were used to analyse device-level observations. Analysis of the analytical framework was performed to investigate if material-level variability can give enough different and repeatable electrical response for hardware fingerprinting and secure key generation.

2.2 Functional Material Parameters

The grain size, film thickness, surface roughness, defect density, porosity, crystallinity, lattice parameter and phase purity were the structural parameters characterized. These parameters were chosen as they can affect charge transport, resistance, the dielectric response, and the switching behaviour of functional electronic materials. The variation of these characteristics between devices was thought to be a possible source of physical uniqueness for hardware-security applications.

2.3 Electrical Characterization

The electrical properties were measured in terms of conductivity, resistance, dielectric constant, leakage current, switching voltage and impedance. These variables are the ones that related to a charge transport, insulating behaviour, switching response, and frequency dependent electrical characteristics. The overall electrical data set was then used to define the response profile of individual devices and to explore the relationship between the response profile and the structural variability.

2.4 Hardware Fingerprint and Key Generation

Structural and electrical variables were normalized to minimize the measurement scale differences. For each device, the response value was then converted to a binary value by using pre-defined threshold-based quantization. The generated binary sequences were merged together to create hardware fingerprints for the individual material and electrical parameters. These fingerprints were then used to create cryptographic key sequences specific to these devices. The key stability and bit balance were tested to check the responses were stable enough for hardware security applications.

2.5 Cryptographic Performance Evaluation

Entropy, inter-device Hamming distance, intra-device reproducibility, bit-error rate, stable key bits, bit balance and uniqueness were used for cryptographic performance evaluation. Increasing entropy and Hamming distance of the devices exhibited more randomness and device differentiation, and increasing key reproducibility and decreasing bit error rate represented better key stability. All of them were combined and assessed to assess whether material-derived fingerprints could be used to generate a secure cryptographic key.

2.6 Quantum-Resistant Hardware Readiness

Combined criteria derived from entropy, uniqueness, reproducibility, bit-error rate and key stability were used to evaluate the readiness of the hardware security. The devices with higher entropy, strong uniqueness, higher

reproducibility, balanced binary response and low error rates were found to be more suitable for integration in quantum resistant hardware security architecture and post quantum cryptographic security systems.

2.7 Statistical Analysis

Structural, electrical and security features were summarized using descriptive statistics. Numerical data were summarised as mean $\pm$ standard deviation or median and interquartile range and categorical data were summarised as frequencies and percentages. Pearson or Spearman correlation was used to assess relationships among variables. Two group comparisons were performed using independent t-tests or Mann–Whitney U tests, and two types of regression (simple linear and simple logistic) were used to investigate predictability of security performance and hardware readiness, respectively. A p value of < 0.05 was considered statistically significant.

2.8 Ethical Considerations

It is not a study with human subjects, animals, personal data or clinical records. As a result, no institutional ethical approval and informed consent were needed. Any engineering or hardware related variable was analysed without collecting or processing any personal details which could identify the sample.

3. Results

3.1 Distribution of Functional Materials and Hardware Readiness

This involved 1,200 observations of devices spread across six classes of functional material. The highest percentage was of PETZ devices (17.42%) followed by HfO₂ memristive oxide (17.25%), PVDF-TrFE polymer (16.92%), TiO₂ memristive oxide (16.75%), BiFeO₃ ferroelectric (15.92%) and graphene based composite devices (15.75%). In total 977 devices (81.42%) were successful in the quantum-resistant hardware-readiness assessment, and 995 devices (82.92%) passed the basic randomness assessment. The results of the distribution of material classes are summarized in Table 1 and illustrated in Figure 1.

Table 1. Distribution of Functional Materials and Security Readiness

Variable	Category	n	%
Functional material	BiFeO ₃ ferroelectric	191	15.92
	Graphene composite	189	15.75
	HfO ₂ memristive oxide	207	17.25
	PVDF-TrFE polymer	203	16.92
	PZT piezoelectric	209	17.42
	TiO ₂ memristive oxide	201	16.75
NIST basic randomness	Passed	995	82.92
Quantum-resistant hardware readiness	Ready	977	81.42

The relatively balanced distribution across the six material classes shown in Figure 1 supported comparative assessment without substantial over-representation of a single functional material type.

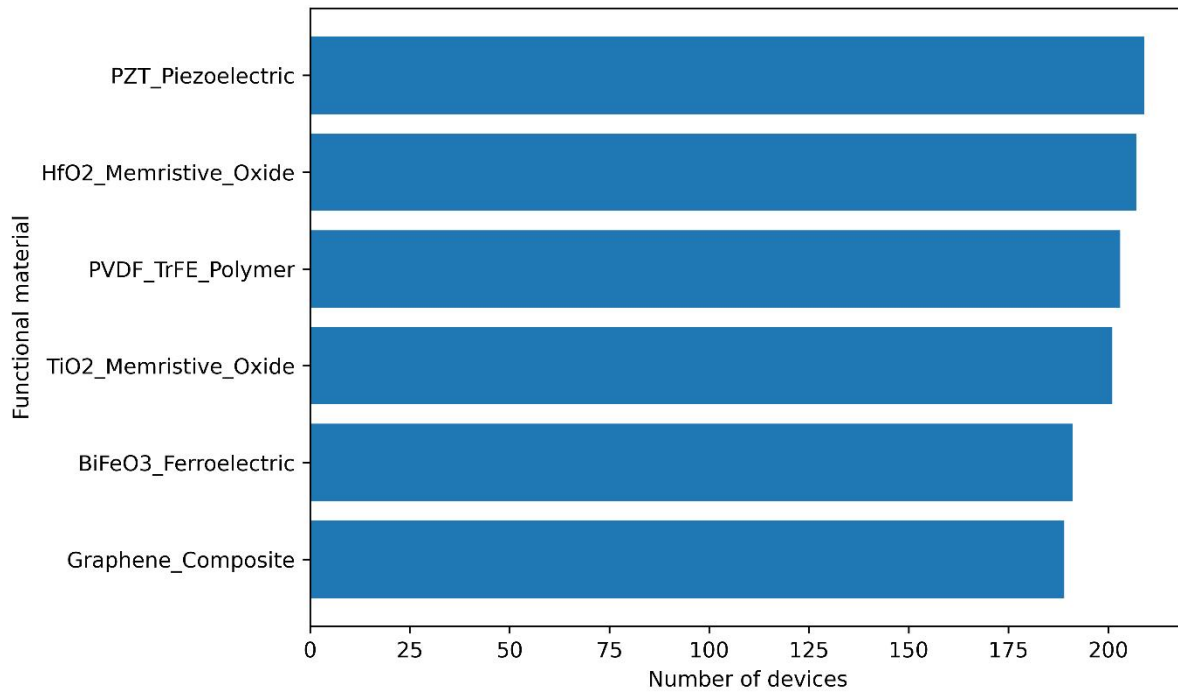


Figure 1. Distribution of Functional Material Classes

3.2 Structural Characteristics of Functional Materials

Entropy, inter-device Hamming distance, intra-device reproducibility, bit-error rate, stable key bits, bit balance and uniqueness were used for cryptographic performance evaluation. Increasing entropy and Hamming distance of the devices exhibited more randomness and device differentiation, and increasing key reproducibility and decreasing bit error rate represented better key stability. They were all brought together and evaluated as a group to determine if material-derived fingerprints can be used to create a secure cryptographic key. Structural Characteristics of Functional Material represented in Table 2.

Table 2. Structural Characteristics of Functional Materials

Structural parameter	Mean $\pm$ SD	Median (IQR)
Film thickness (nm)	141.75 $\pm$ 128.95	88.24 (78.83–100.74)
Grain size (nm)	32.75 $\pm$ 24.68	22.98 (12.77–46.09)
Surface roughness (nm)	10.43 $\pm$ 6.57	9.02 (4.46–14.24)
Defect density (cm ⁻²)	3.23 $\times 10^{-7} \pm 2.04 \times 10^{-7}$	2.64 $\times 10^{-7}$ (1.70–4.15 $\times 10^{-7}$)
Porosity (%)	5.74 $\pm$ 1.37	5.76 (4.80–6.65)
Crystallinity (%)	77.81 $\pm$ 4.73	77.71 (74.49–81.03)
Lattice parameter (Å)	4.243 $\pm$ 0.053	4.244 (4.207–4.281)
Phase purity (%)	89.14 $\pm$ 2.30	89.10 (87.62–90.57)
Structural variability index	3.42 $\pm$ 1.00	3.17 (2.81–3.75)

3.3 Electrical Response Characteristics

There were significant variations in electrical measurements between devices. Mean electrical conductivity was $294,352.40 \pm 173,115.10$ S/m, while resistance had a median value of 3.18 k Ω . Mean dielectric constant was 39.45 ± 7.53 and switching voltage was 1.28 ± 0.14 V. Leakage current remained low at 0.70 ± 0.10 μ A. Impedance had a very broad distribution, with median of 1,355.36 Ω and a mean of 6,237.91 Ω . The following electrical characteristics are shown in Table 3.

Table 3. Electrical Characteristics of Functional Material Devices

Electrical parameter	Mean $\pm$ SD	Median (IQR)
Electrical conductivity (S/m)	$294,352.40 \pm 173,115.10$	273,142.60 (161,159.05–403,611.88)
Resistance (k Ω)	12.87 ± 22.87	3.18 (2.07–5.43)
Dielectric constant	39.45 ± 7.53	39.03 (34.13–44.71)
Switching voltage (V)	1.282 ± 0.141	1.275 (1.184–1.378)
Leakage current (μ A)	0.701 ± 0.104	0.698 (0.634–0.766)
Impedance at 1 MHz (Ω)	$6,237.91 \pm 11,498.76$	1,355.36 (815.35–2,546.37)
Temperature coefficient (ppm/ $^{\circ}$ C)	178.73 ± 29.78	178.20 (158.52–198.55)
Electrical variability index	2.09 ± 0.60	1.99 (1.63–2.46)

3.4 Cryptographic Key-Generation Performance

The resulting hardware fingerprints were found to have very good security properties. The Mean PUF uniqueness is $48.74 \pm 1.86\%$ and the inter-device Hamming distance is $48.69 \pm 2.18\%$, which is very close to the ideal 50% differentiation level. The PUF reproducibility is high ($97.30 \pm 0.50\%$) and the mean stable-key rate is 97.29%. The Shannon entropy was 0.963 bit/bit and the mean minimum entropy was 0.953 bit/bit. Key bit-error rate remained low at $2.71 \pm 0.54\%$ (Table 4).

Table 4. Cryptographic and Hardware-Fingerprint Performance

Security metric	Mean $\pm$ SD	Median (IQR)
PUF uniqueness (%)	48.74 ± 1.86	48.75 (47.44–50.06)
PUF reproducibility (%)	97.30 ± 0.50	97.28 (96.94–97.60)
Bit balance (%)	49.91 ± 2.06	49.95 (48.51–51.28)
Intra-device Hamming distance (%)	2.70 ± 0.63	2.70 (2.29–3.13)
Inter-device Hamming distance (%)	48.69 ± 2.18	48.76 (47.17–50.15)
Shannon entropy (bit/bit)	0.963 ± 0.010	0.963 (0.957–0.970)
Minimum entropy (bit/bit)	0.953 ± 0.010	0.953 (0.946–0.960)
Key bit-error rate (%)	2.71 ± 0.54	2.74 (2.35–3.09)
Stable-key rate (%)	97.29 ± 0.55	97.27 (96.88–97.66)

Key lengths of 128, 256, and 512 bits were represented by 240, 735, and 225 devices, respectively, demonstrating that the evaluated fingerprint framework supported multiple cryptographic key sizes.

3.5 Relationships Between Material Variability and Security Performance

The variation of structural variability was strongly positively correlated with PUF uniqueness ($\rho = 0.196$), PUF reproducibility ($\rho = 0.348$) and Shannon entropy ($\rho = 0.253$) and negatively correlated with key bit-error rate ($\rho = -0.335$). There were similar but less strong relationships for electrical variability with uniqueness ($\rho = 0.161$), with reproducibility ($\rho = 0.215$), and with entropy ($\rho = 0.159$). The results of the correlation patterns are summarized in Table 5 and illustrated in Figure 2.

Table 5. Spearman Correlations Between Variability and Cryptographic Performance

Variables	ρ	p-value
Structural variability – PUF uniqueness	0.196	<0.001
Structural variability – PUF reproducibility	0.348	<0.001
Structural variability – Shannon entropy	0.253	<0.001
Structural variability – key bit-error rate	-0.335	<0.001
Electrical variability – PUF uniqueness	0.161	<0.001
Electrical variability – PUF reproducibility	0.215	<0.001
Electrical variability – Shannon entropy	0.159	<0.001
Electrical variability – key bit-error rate	-0.206	<0.001
PUF uniqueness – Shannon entropy	0.732	<0.001
PUF reproducibility – key bit-error rate	-0.925	<0.001

As shown in Figure 2, PUF uniqueness was strongly associated with Shannon entropy, whereas reproducibility demonstrated a very strong inverse relationship with bit-error rate. These patterns indicate that more stable device responses were accompanied by lower key-generation errors.

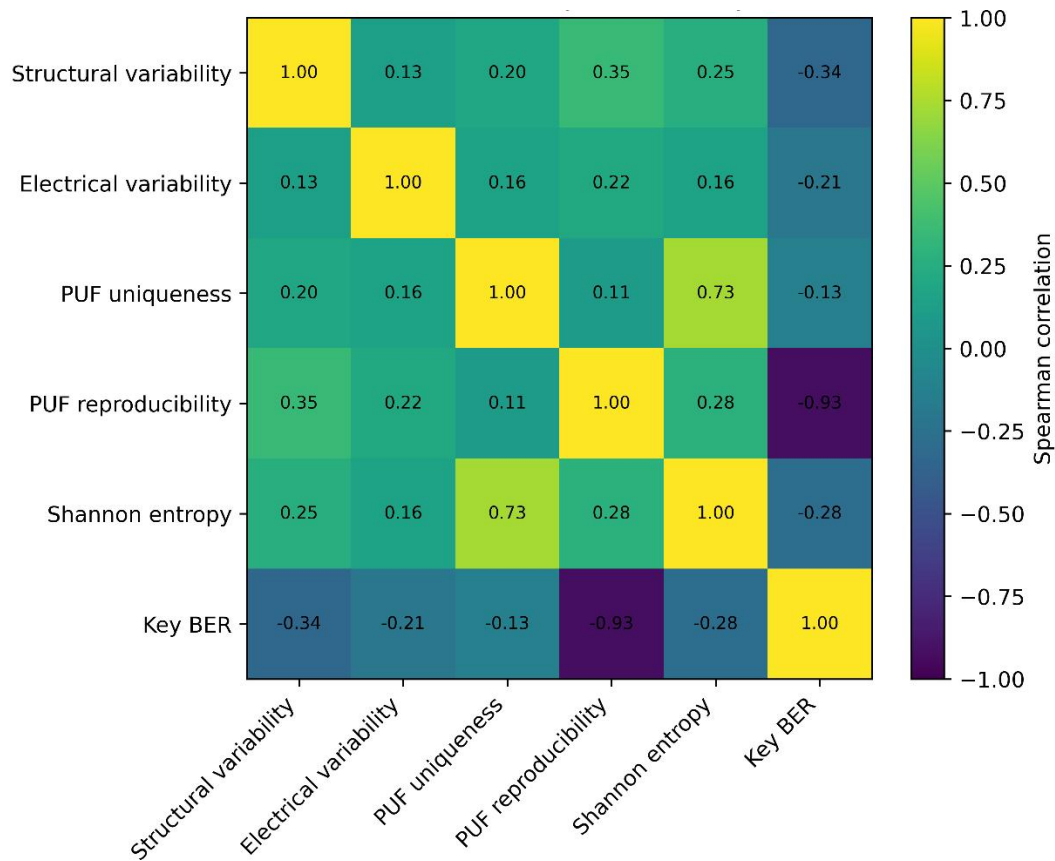


Figure 2. Correlation Matrix of Structural, Electrical, and Cryptographic Performance Variables

3.6 Quantum-Resistant Hardware Readiness

The quantum resistant hardware ready devices were found to perform much better on both material-variability and cryptographic metrics. A higher structural and electrical variability index, a higher PUF uniqueness and reproducibility, a higher inter-device Hamming distance and a higher entropy were observed for the ready devices. The average key bit error rate (BERT) was also lower at 2.66% for their devices versus 2.93% for devices that were not ready. Each of the group differences selected were statistically significant as shown in Table 6.

Table 6. Comparison of Quantum-Resistant Hardware-Ready and Non-Ready Devices

Variable	Ready, mean $\pm$ SD	Not ready, mean $\pm$ SD	p-value
Structural variability index	3.47 $\pm$ 1.04	3.22 $\pm$ 0.77	<0.001
Electrical variability index	2.12 $\pm$ 0.61	1.98 $\pm$ 0.55	0.002
PUF uniqueness (%)	48.99 $\pm$ 1.72	47.64 $\pm$ 2.06	<0.001
PUF reproducibility (%)	97.34 $\pm$ 0.49	97.09 $\pm$ 0.52	<0.001
Inter-device Hamming distance (%)	48.95 $\pm$ 2.03	47.54 $\pm$ 2.44	<0.001
Shannon entropy (bit/bit)	0.965 $\pm$ 0.008	0.955 $\pm$ 0.011	<0.001
Minimum entropy (bit/bit)	0.955 $\pm$ 0.009	0.944 $\pm$ 0.010	<0.001
Key bit-error rate (%)	2.66 $\pm$ 0.52	2.93 $\pm$ 0.57	<0.001

Stable-key rate (%)	97.34 ± 0.53	97.08 ± 0.58	<0.001
---------------------	------------------	------------------	----------

The relationship between structural and electrical variability according to hardware-readiness status is illustrated in Figure 3. Ready devices were distributed across the full variability range, although their mean structural and electrical variability indices were significantly higher than those of non-ready devices.

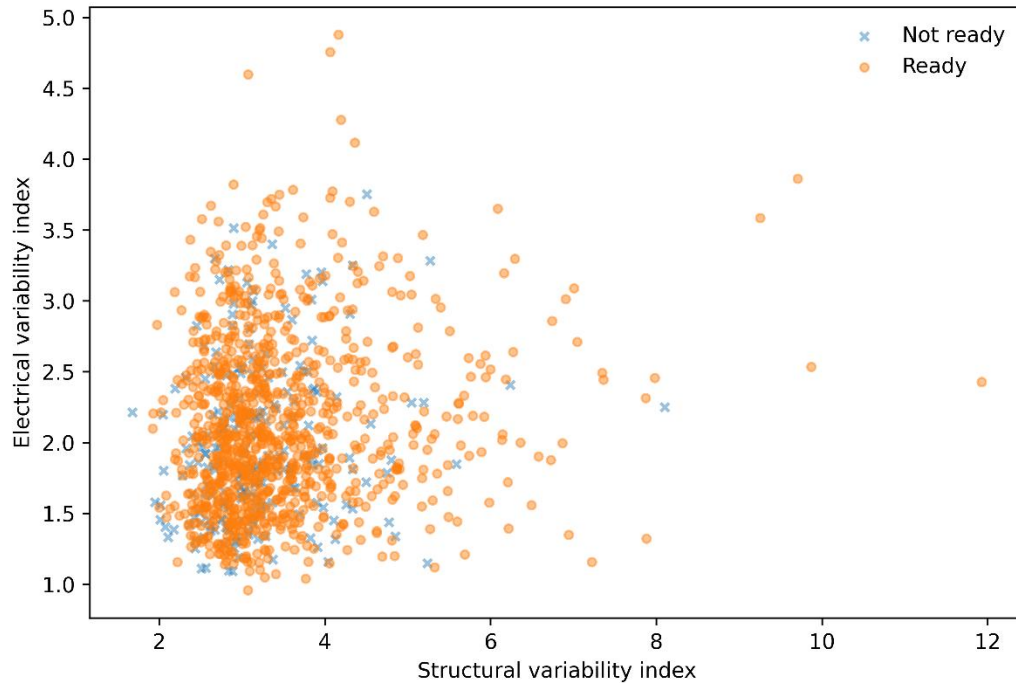


Figure 3. Structural and Electrical Variability According to Quantum-Resistant Hardware Readiness

3.7 Entropy Performance According to Hardware Readiness

One of the most distinct differences between readiness groups was Shannon entropy. The mean Shannon entropy value of devices that met the quantum-resistant hardware-readiness criterion was 0.965 ± 0.008 bit/bit, versus 0.955 ± 0.011 bit/bit for the non-ready devices ($p < 0.001$).

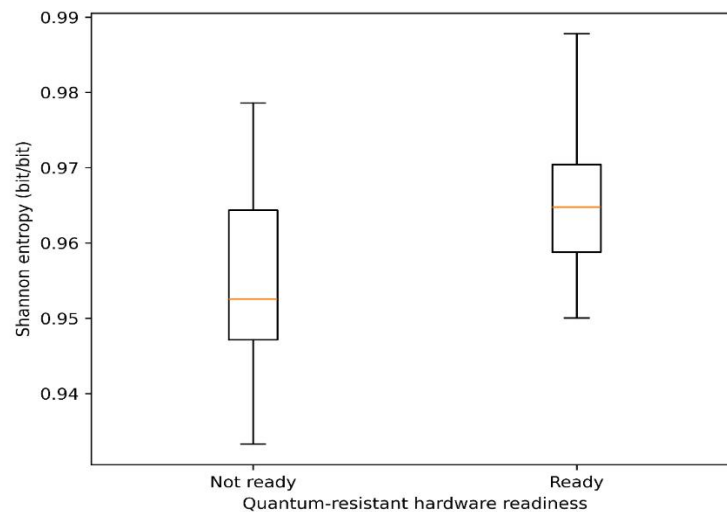


Figure 4. Shannon Entropy Distribution by Quantum-Resistant Hardware Readiness

The distribution presented in Figure 4 shows a consistent upward shift in entropy among hardware-ready devices, supporting the relationship between improved randomness characteristics and overall cryptographic readiness.

4. Discussion

The present study showed that the structural and electrical fluctuations of functional materials can serve as a practical means for cryptographic key generation based on hardware. The measured devices exhibited significant variations in grain size, film thickness, surface roughness, defect density, crystallinity, conductivity, resistance, impedance and switching characteristics. These variations were observed to be accompanied by good cryptographic characteristics as the PUFs were characterised by high PUF reproducibility, near-balanced bit distributions, high entropy and inter device Hamming distances near the ideal value for device differentiation. This is important to support the current efforts of implementing physical characteristic of the hardware with quantum resilient architectures for authentication and key generation, which is distributed between the hardware and cryptographic layers and not only protected by software-based protection (Alsayaydeh et al., 2025).

One result that was very significant was the positive association between structural variability and cryptographic performance. The more variable the structure the more unique and reproducible it was, and the more Shannon entropy it exhibited, but the less key bit-error rate. This means that some degree of heterogeneity in the material on a controlled level may enhance electrical signatures on a device level without necessarily reducing the stability of the response. The hardware-based identity is more important for quantum resistant authentication systems, especially for the identification of a node in a distributed digital system (Alutaoui, 2025). A parallel scenario can be seen in the context of connected vehicle architectures, where protection of the stored data is needed in addition to network security with hardware awareness, to reduce the vulnerability to new threats (Castiglione & Elia, 2025).

The relationship of electrical variability was also positive to uniqueness and entropy but was less than the relationship for structural variability. This means that electrical behaviour can serve as a measurable output which maps the underlying differences in materials to a Security relevant fingerprint. The excellent repeatability found in the current analysis is particularly significant as the key from the hardware needs to be quite stable when repeated measurements are made. Efficient post-quantum protection is also a key priority in hardware implementations, such as those using RISC-V and other embedded architectures (Dolmeta, 2025). This holds true for communication systems on UAVs as well, where communication devices are subject to extensive hardware and communication restrictions, and secure authentication and key establishment still need to be conducted (Epure, 2025). Moreover, for quantum-resistant authentication, practical implementations focused on performance show that besides selecting the algorithm, efficient hardware implementation is crucial for security (Fraile et al., 2025).

The results obtained for the mean entropy and key-stability have also shown the potential use of material variability as a physical source to derive cryptographic keys. This is different from the approach of software generated keys, which get their entropy from the software. Some works on latent-key generation have demonstrated that using unique physical or encoded responses in conjunction with quantum-resilient security mechanisms can be rewarding (Gangappa & Satyanarayana, 2025). Biometric cryptographic systems have also shown that complex physical properties can be used to generate cryptographic key material as long as the variability and repeatability are maintained (Kuznetsov et al., 2024). These are mechanisms that can be implemented through hardware and might be especially useful in resource-limited consumer electronics, where post-quantum algorithms can cause extra computational and memory requirements (Khan et al., 2025).

The majority of devices in the current study met the criteria for quantum-resistant hardware-readiness and the ready devices were shown to have significantly increased entropy, uniqueness, reproducibility, and stable-key rates, and lower error rates. These characteristics apply to connected medical devices where long-term integrity and secure device authentication is paramount (Kothapalli, 2025). They can also be used in blockchain-based systems, where quantum-resistant algorithms are an emerging feature to ensure secure authentication, transactions, and distributed records (Samonte & Asuncion, 2025). There have been suggestions of such integration with financial blockchain services (Samonte et al., 2024), privacy focused biomedical ecosystems (Subramanian et al., 2025), and IoT banking infrastructures (Tumma et al., 2025).

The results suggest a possible additional hardware-based root of trust for QKD, which can be combined with post quantum cryptographic algorithms. This could boost device authentication, key generation and cloning resistance, and be compatible with overall quantum resistant architectures. Performance analysis of quantum-resistant

blockchain systems also highlights the necessity of considering both the security benefits and computational and implementation efficiency (Wu et al., 2025). Future research should thus confirm these correlations in real devices over a range of temperatures, aging, cycling, and under adverse conditions, to ensure long-term reliability and pragmatic compatibility with post-quantum cryptographic hardware devices.

5. Conclusion

This work revealed that structural and electrical fluctuation of functional material has the potential to form a solid physics basis for generating cryptographic key in quantum resistant hardware. Different values of these grain sizes, film thicknesses, surface roughness, defect density, crystallinity, conductivity, resistance, impedance and switching behaviour led to different electrical responses from the devices at the hardware level which could be used as hardware fingerprints. Material-derived variability successfully provided stable and distinguishable cryptographic responses as the resulting security characteristics demonstrated strong uniqueness, high reproducibility, near-balanced binary responses, high entropy and low bit-error rates. Both structural and electrical variability exhibited particularly significant relationships with uniqueness, reproducibility, entropy and key stability. Hardware-ready devices also exhibited better cryptographic capabilities such as higher entropy, better difference between devices, higher stable key rates, and lower levels of error. These results can be used to build functional materials for physical entropy sources and hardware roots of trust that can be used in conjunction with post quantum cryptographic algorithms. The proposed approach is an interdisciplinary approach that links materials engineering and post-quantum hardware security. Randomness at the material level can enhance authentication, key generation, cloning resistance, and more in embedded and connected systems. More experimental testing is needed under the conditions of temperature variation, aging, frequent switching, fabrication variations and adversarial conditions before being realized in secure hardware resistant to quantum computers.

References

1. Alsayaydeh, J. A. J., Yusof, M. F., Yahaya, N. A., Kovtun, V., & Herawan, S. G. (2025). A novel framework for secure cryptocurrency transactions using quantum crypto guard. *PeerJ Computer Science*, 11, e3030.
2. Alutaibi, A. I. (2025). Quantum-resilient blockchain for secure digital identity verification in DeFi. *Computers, Materials & Continua*, 85(1), 875-903.
3. Bhatia, A., Bitragunta, S., & Tiwari, K. (2025). PUF-AQKD: A hardware-assisted quantum key distribution protocol for man-in-the-middle attack mitigation. *IEEE Open Journal of the Communications Society*, 6, 4923-4942.
4. Bishwas, A. K., & Sen, M. (2024). Strategic roadmap for quantum-resistant security: A framework for preparing industries for the quantum threat. *arXiv preprint arXiv:2411.09995*.
5. Carroll, T. E., Moran-Schmoker, A. M., & Redington, L. M. (2024). Exploring the adoption challenges of post-quantum cryptography in EV charging infrastructure. Dept. Pacific Northwest National Laboratory, Richland, WA, USA, Tech. Rep, 35760.
6. Castiglione, A., & Elia, T. (2025). Securing in-vehicle communications through post-quantum cryptography and network segmentation. *Computers and Electrical Engineering*, 126, 110488.
7. Chowdhury, S., Covic, A., Acharya, R. Y., Dupee, S., Ganji, F., & Forte, D. (2020). Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. *arXiv preprint arXiv:2005.04344*.
8. Dolmeta, A. (2025). A Post-Quantum Secure RISC-V application core for IoT: from hardware design to applications.
9. Epure, L. I. (2025). Post-Quantum Cryptography for Military UAV Communication Systems A Comprehensive Framework for Quantum-Resistant Security in MAVLink-Based Unmanned Aerial Vehicles.
10. Fraile, L. P., Tasopoulos, G., Koulamas, C., Zhao, R. K., Sultan, N. H., Regazzoni, F., & Fournaris, A. P. (2025). Enabling quantum-resistant edhoc: Design and performance evaluation. *IEEE Access*, 13, 75861-75884.
11. Gangappa, M., & Satyanarayana, B. V. (2025). Secure Image Transmission using Quantum-Resilient and Gate Network for Latent-Key Generation. *Journal of Electronics, Electromedical Engineering, and Medical Informatics*, 7(4), 1178-1198.

12. Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials*, 26(3), 1748-1774.
13. He, Z., Elizarov, M. S., Li, N., Xiang, F., & Fratalocchi, A. (2024). Quantum-activated neural reservoirs on-chip open up large hardware security models for resilient authentication. *arXiv preprint arXiv:2403.14188*.
14. Khan, M. A., Noor, F., Javaid, S., & Żywiołek, J. (2025). Implementation and performance of post-quantum cryptography for resource constrained consumer electronics. *Discover Internet of Things*, 5(1), 139.
15. Kothapalli, S. D. (2025). A Quantum-Resilient Blockchain Architecture for Long-Term Integrity and Secure Authentication of Connected Medical Device Data. Available at SSRN 7414058.
16. Kuznetsov, O., Zakharov, D., & Frontoni, E. (2024). Deep learning-based biometric cryptographic key generation with post-quantum security. *Multimedia Tools and Applications*, 83(19), 56909-56938.
17. Mattsson, J. P., Smeets, B., & Thormarker, E. (2021). Quantum-resistant cryptography. *arXiv preprint arXiv:2112.00399*.
18. Mougkogiannis, P., Ghadafi, E., & Adamatzky, A. (2025). Bio-inspired cryptography based on proteinoid assemblies. *PLoS One*, 20(5), e0324761.
19. Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in post-quantum era: A comprehensive survey on lattice-based algorithms. *IEEE access*, 13, 89003-89024.
20. Nieto-Morales, A., Bishwas, A. K., & Varghese, J. J. (2025). Quantum-enabled framework for the Advanced Encryption Standard in the post-quantum era. *arXiv preprint arXiv:2502.02445*.
21. Samonte, M. J. C., & Asuncion, K. D. R. (2025). Quantum-Resistant Cryptographic Algorithms for Blockchain Integration. *Information Systems for Intelligent Systems: Proceedings of ISBM 2024, Volume 2*, 2, 425.
22. Samonte, M. J. C., Asuncion, K. D. R., Castillo, J. J. A. G., & Santos, H. H. I. (2024, September). Quantum-Resistant Cryptographic Algorithms for Blockchain Integration in Financial Services. In *World Conference on Information Systems for Business Management* (pp. 425-439). Singapore: Springer Nature Singapore.
23. Srinivas, M. B., & Elango, K. (2024). Era of sentinel tech: Charting hardware security landscapes through post-silicon innovation, threat mitigation and future trajectories. *IEEE Access*, 12, 68061-68108.
24. Subramanian, S., Malarvizhi, C., Nadhiya, S., Siva, K. P., Ayyavu, P. G., & Alagarsamy, M. (2025, November). Quantum-Resistant Hashing for Protecting Genomic Privacy within Decentralized Biomedical Data Ecosystems. In *2025 International Conference on Electrical Engineering and Informatics (ICEEI)* (pp. 1-8). IEEE.
25. Tumma, C., Ayyamgari, S., Sannapu, R., Srihashyam, A. S., & Kadari, S. (2025, November). Quantum-resistant cryptographic architecture for secure payments and iot-driven banking ecosystems. In *2025 38th Conference of Open Innovations Association (FRUCT)* (pp. 291-297). IEEE.
26. Turnip, T. N., Andersen, B., & Vargas-Rosales, C. (2025). Toward 6G authentication and key agreement protocol: A survey on hybrid post quantum cryptography. *IEEE Communications Surveys & Tutorials*, 28, 3311-3345.
27. Vermeer, M. J., Heitzenrater, C., Parker, E., Moon, A., Lumpkin, D., & Awan, J. (2024). Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems. *Journal of Critical Infrastructure Policy*, 5(2), 88-110.
28. Wu, F., Zhou, B., Song, J., & Xie, L. (2025). Quantum-resistant blockchain and performance analysis. *The Journal of Supercomputing*, 81(3), 498.
29. Yusof, N. A. M., Azni, A. H., Ridzuan, F., Zakaria, N. H., Pitchay, S. A., Zakaria, A. A., & Ali, T. (2025). Toward Quantum-Resilient PKI: A Systematic Literature Review of Post-Quantum Certificates Model. *Malaysian Journal of Science Health & Technology*, 76-85.
30. Zhang, K., Yang, M., Yuan, Z., Zhang, Y., & Liu, W. (2025). Optimized quantum-resistant cryptosystem: integrating Kyber-KEM with hardware TRNG on Zynq platform. *Electronics*, 14(13), 2591.