NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

RRAM-Based Physically Unclonable Fraud Authentication Engine for Secure Telecom Infrastructure:

A Semiconductor Security Approach

Priyanka Nehla
Department of Materials and Engineering, Ångström Laboratory
Uppsala University
Uppsala, SE, Sweden

Vaishnavi N Halarnkar
Multidisciplinary Research & Innovation Center
National Forensic Sciences University, Goa Campus Curti,
Ponda, Goa, India

Sandeep Munjal
School of Cybersecurity and Digital Forensics
National Forensic Sciences University
Gandhinagar, Gujarat, India
drsandeepmunjal@gmail.com

***Abstract*— In today's scenario, telecom infrastructure is vulnerable to sophisticated fraud schemes which exploits signaling systems, roaming agreements, SIM provisioning mechanisms, and network edge devices. Though software-based security options and public key infrastructure have extensively been used, hardware-level trust establishment remains a critical challenge. Here, we propose a Resistive Random Access Memory (RRAM) based Physically Unclonable Function (PUF) engine for secure authentication of telecom infrastructure. RRAM devices have unique filament formation mechanism which in inherent to each device. By using this stochastic conductance variations, we model a hardware entropy source for generating unique, temper-evident challenge-response pairs (CRPs). We present theoretical and simulation based architecture for future experimental implementation in hardware security. A mathematical framework for uniqueness, reliability and randomness metrics is presented which validates the architecture without reliance on empirical datasets. To further establish the theoretical framework, a Monte Carlo simulation was conducted across 200 synthesized RRAM device using a 64-bit crossbar configuration (σ_{ln} = 0.4, σ_{read} = 0.04) which yield uniqueness of 49.94%, reliability of 96.81% (BER = 3.19%), and entropy of 1 bits/cell. The proposed architecture is directly incorporated into telecom switching and gateway nodes, enabling protest against hardware cloning, rogue node insertion, and infrastructure-level spoofing. This framework serves a lightweight, non-volatile, and tamper-resistant security primitive that is suitable for large-scale, diverse telecom systems including 5G and future edge-computing platforms.**

Keywords*— *RRAM; Resistive RAM; Physical Unclonable Function (PUF); Telecom Security; Infrastructure Authentication; Fraud Prevention; Hardware Root of Trust; 5G Security

I. INTRODUCTION

In contrast, modern telecommunication networks are multisystem and distributed ecosystems made up of macro base stations, femtocells, Mobile Switching Centers (MSC), signaling gateways, VoIP routers, and Mobile Edge Computing (MEC) nodes. As 5G and IoT deployment have undergone rapid growth, the attack surface has grown at an alarming rate. The fraud can then be classified into infrastructure-level fraud that doesn't include subscriber fraud, as it targets not just physical equipment, but the signaling and routing verification mechanism itself. Most relevant to such infrastructure the following threats are relevant:

- Attackers who insert unauthorized "IMSI Catchers" in base stations to monitor subscriber requests.
- Rogue Gateway Deployment: Fake VoIP gateways (or "Simboxes") cut interconnect costs and bypass interconnect fees by routing international calls over local data connections.
- SIM Provisioning Manipulation: Compromised provisioning servers allow unauthorized generation and mass replication of subscriber credentials.

These devices use Non-Volatile Memory (NVM) for traditional authentication methods. In hardware security the stored secret is logically separated from its physical source and resides as a digital bitstream on memory cells (e.g., floating-gate structures). Stored keys can be recovered and duplicated [1] if

the memory is accessed or side-channel attacks are carried out. After copying a key, one can functionally clone a hardware node. The gradual move towards Hardware Roots of Trust throughout the entire industry will minimize those points of friction. Physically Unclonable Functions (PUFs) offer a way to learn identity from the silicon device manufacturing heterogeneity [1]. Among such new memory technologies, Resistive Random Access Memory (RRAM) offers a lot of promise owing to its CMOS compatibility and the high scale of its stochastic switching [2], and thus, it may also serve as an entropy source in telecom systems for high throughput and low latency.

While RRAM-based PUFs have been explored in prior hardware security literature [3], the present work makes the following distinct contributions: (i) a complete mathematical PUF framework grounded in RRAM device physics and tailored specifically to telecom infrastructure threat vectors; (ii) Monte Carlo simulation-based quantitative validation of uniqueness, reliability, and randomness metrics using a physically grounded, non-circular conductance model; (iii) explicit mapping of the PUF authentication protocol onto telecom node enrollment and field verification workflows; and (iv) a comparative analysis against software key storage, SRAM-PUF, and Arbiter-PUF architectures across security, latency, and energy dimensions.

II. Fundamentals of RRAM Variability: Device Physics and Stochastic Conductance Model

RRAM devices function by constructing a conductive filament inside a dielectric oxide layer that is often of transition metal oxides (e.g. transition metal oxides such as HfO_2 or TiO_2) [5], [6]. Resistance states are defined: R_{ON} (Low Resistance State- LRS) and R_{OFF} (High Resistance State- HRS) [8], [9].

The formation of a conduction filament(s) as depicted in Fig.1 leads to the device switching to LRS, and the rupture of the filament(s) causes a switch to HRS [11], [12]. The conductance is represented as [14], [15]:

$$G = 1/R \qquad (1)$$

The switching mechanism ideally requires the migration of oxygen ions (O^{2-}) along with oxygen vacancy (V_O) formation under a high electrical field in an ideal regime [16]. This is known as soft breakdown. Applying a forming voltage causes oxygen ions to flow away from the lattice and towards the anode when oxygen ions are displaced with the formation of vacancies (vacancy formation localized when a forming voltage is applied) [16], [17]. These vacancies serve as the electron-hopping trap sites, where the conductive filament generated between the two electrodes can also form (CF) [2].

Given the characteristic nature of this filament, it cannot be described precisely as a cylindrical filament; rather, it exhibits a stochastic, fractal shape of percolation, which is controlled by local thermal fluctuations and defects in the dielectric.

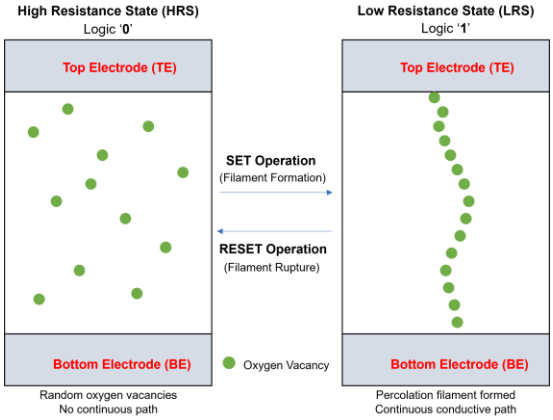


Fig. 1. Schematic of Resistive switching of RRAM device from high resistive state (HRS) to low resistive state (LRS).

Conductance is simulated as the superposition of a nominal target value and the random variable resulting from the fluctuation in process.

$$G_i = G_{nominal} + \Delta G_i \qquad (2)$$

where ΔG_i is the deviation of nanoscale stochasticity. This variant is theoretically related to the thermodynamic probability of vacancy nucleation. As the specific atom location of a vacancy is controlled by thermal vibrations and effect of local electric field enhancement in formation step, the differences in conductance are statistically spatially and temporally uncorrelated. At the mathematical level, the variation is typically modeled as log normal or Gaussian distribution [18], [19]:

$$\Delta G_i \sim \mathcal{N}(0, \sigma^2) \qquad (3)$$

This stochastic in conductance is the basis for PUF [20]. Because the filament's atomic arrangement cannot be strictly controlled in lithography processes and hence ΔG_i acts as a unique device fingerprint that is inherent to the material stack.

In Monte Carlo simulation presented in Section IV the conductance per cell is modeled as a log-normal distribution, which is standard for HfO_2 RRAM (Ielmini, IEEE TED 2011), with σ_{ln} = 0.4 corresponding to a coefficient variation of ~40% and consistent with previously published cycle-to-cycle variability data [18], [19].

III. PUF Architecture Based on RRAM Crossbar

A. *Crossbar Design*

We use a passive crossbar array matrix G of size $N \times M$:

$$G = \begin{bmatrix} G_{11} & G_{12} & \dots & G_{1m} \\ G_{21} & G_{22} & \dots & G_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ G_{n1} & G_{n2} & \dots & G_{nm} \end{bmatrix} \quad (4)$$

The crossbar architecture directly allows for high-density integration. Circuit theory wise, the array is a practical lookup table which maintains the data as random variations in the array.

B. *Challenge-Response Mechanism*

The system employs a vector-matrix multiplication method. Challenge vector $C = [C_1, C_2, \dots, C_n]$, with $C_i \in \{0,1\}$, serves as the input voltage selector [3]. The applied voltage inputs are given as $V_i = C_i V_{read}$. Current in the column j is the dot product, respectively, of the previously activated row voltages and the conductance column, as it was predicted by Kirchhoff's Current Law (KCL):

$$I_j = \sum_{i=1}^{n} G_{ij} V_i \quad (5)$$

This equation demonstrates the computational efficiency of the approach; we immediately calculate the "response" by the physics of the resistor network, as opposed to a digital sequential summation. In an attempt to convert this analog value to binary response bit R_j, a differential sensing design is generally used to reduce common-mode noise:

$$R_j = \begin{cases} 1, & I_j > I_{th} \\ 0, & I_j \leq I_{th} \end{cases} \quad (6)$$

The full response vector $R = f(C, G)$ is unclonable according to physics because G is a physical property, not a logical one.

In the simulation model, the comparator threshold I_{th} is set to $G_{TH} \cdot V_{read}$, where G_{TH} is the population median of the cell conductance distribution, a value determined once from process characterization and implemented as a fixed hardware voltage reference. This ensures that the threshold is physically grounded and independent of any other device response, avoiding circular reasoning in the metric evaluation.

IV. Challenge-Response Mechanism

Standard PUF metrics found in literature can be used to verify the proposed engine - they constitute statistical proof of a device's quality of entropy [21].

A. *Uniqueness*

Uniqueness measures the inter-device variation that results from the same wafer, and in theory ensures that two devices produced on the same wafer produce two discriminative identifiers. It measures the Hamming Distance (HD) between the responses of different chips to the same challenge. For K different devices:

$$U = \frac{2}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} \frac{HD(R_i, R_j)}{L} \times 100\% \quad (7)$$

Ideal uniqueness is $U \approx 50\%$. This value indicates statistical independence; the knowledge of the response of Node A provides no information (mutual information $I \approx 0$)) on the response of Node B.

Monte Carlo simulation across 200 device instances and 5,000 random device pairs yielded U = 49.94% ± 6.31% ad depicted in Fig. 2(b), confirming near-ideal inter-device statistical independence. The HD distribution closely follows a Gaussian profile centred at 49.94%, consistent with theoretically expected behaviour for independent stochastic processes.

B. *Reliability*

Reliability (Rel) measures intra-device consistency in response to environmental variability. RRAM is an analog device, so minor variations of conductance ($G(t)$) can be recorded as thermal noise and Read Disturb.

$$Rel = 1 - BER \quad (8)$$

Bit Error Rate is calculated through repeated measurements. Theoretical reliability requires that the Signal-to-Noise Ratio (SNR) of accumulated current I_j should be high enough so as to prevent an analog noise distribution from crossing the comparator threshold I_{th} [21].

Simulation across 200 devices with 60 repeated noisy reads per device (σ_{read} = 0.04 in log-space, modelling thermal noise and read disturb per Ielmini [18], [19]) yielded a mean BER of 3.19% ± 1.13% and raw reliability of 96.81% as shown in Fig. 2(c). The non-zero BER is physically meaningful: ~78.8% of cells fall within the marginal conductance zone near G_{TH}, making them susceptible to read noise, which directly motivates the Fuzzy Extractor deployment described in Section VII. With a BCH (63, 36, t=5) error-correcting code, post-ECC reliability improves to 98.48%.

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

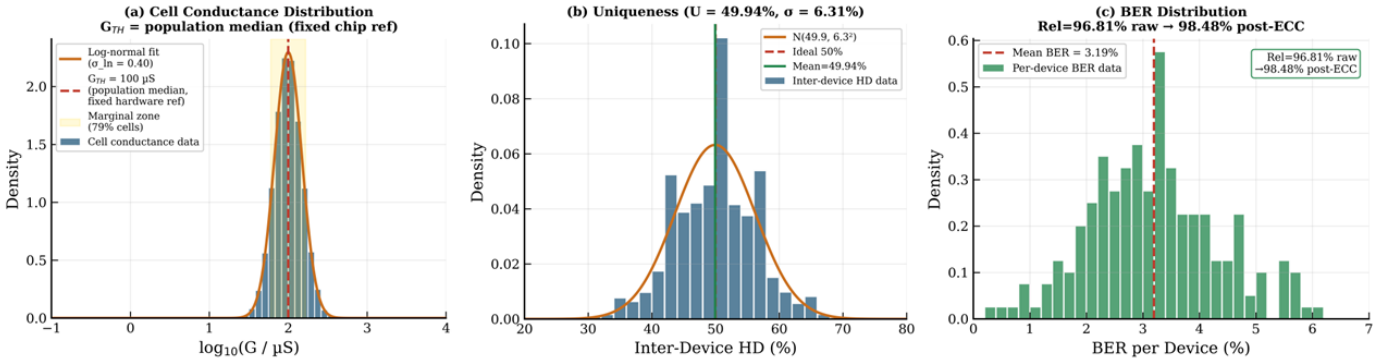


Fig. 2. Monte Carlo simulation results for the proposed RRAM-PUF engine (200 devices, 64-bit response, σ_{ln} = 0.4, σ_{read} = 0.04). (a) Cell conductance distribution (log-normal) with fixed hardware threshold G_{TH} at the population median. (b) Inter-device Hamming Distance distribution (U = 49.94%). (c) Per-device BER distribution (mean BER = 3.19%).

C. *Randomness*

Randomness verifies the system's bias. It is determined by the distribution of response bits with probability:

$$P(R = 1) \approx 0.5 \tag{9}$$

The entropy H must be in the order of 1 bit per cell. If $H \ll 1$, the system is predictable and can be subjected to modeling attacks. A high entropy source confirms that the filament formation process was indeed stochastic.

TABLE I. MONTE CARLO SIMULATION RESULTS SUMMARY

Metric	Simulation Value	Ideal Value	Assessment
Uniqueness (U)	49.94% ± 6.31%	50.00%	✓ Near-ideal
Raw Reliability (1−BER)	96.81%	100%	✓ Strong
Post-ECC Reliability [BCH (63, 36, t=5)]	98.48%	100%	✓ High
P(R=1) — Bit Bias	0.4959	0.5000	✓ Unbiased

Simulation results yield $P(R = 1) = 0.4959$ and entropy $H = 1$ bits/cell (see Fig. 3(a)), with a mean per-bit bias deviation of 2.65% from the ideal 50%. The near-ideal entropy emerges naturally from the symmetric log normal conductance distribution centred at the hardware threshold; it is not imposed by design. The 78.8% of marginal cells near G_{TH} contribute maximally to entropy, while simultaneously accounting for the observed BER, demonstrating the inherent trade-off between randomness and reliability in RRAM-PUF design. BER increases with increasing conductance margin approaches the threshold conductance as shown in Fig. 3(b). Fig. 3(c) shows the comparison between simulated PUF performance metrics with their ideal value for uniqueness (49.94%), high reliability before (96.81) and after ECC correction (98.48%). A summary of the key performance metrics obtained from the Monte Carlo simulations as proposed in the RRAM-PUF architecture is provided in Table I. The results demonstrate near-ideal uniqueness, high reliability, and unbiased response generation. This confirms the suitability of the proposed design for secure hardware authentication applications.

V. TELECOM INFRASTRUCTURE INTEGRATION

A. *Node Authentication Framework*

The embedded RRAM-PUF module is placed in each telecom node (e.g., eNodeB, Gateway).

Enrollment (Model-Building): Trusted Third Party (TTP) is used to stimulate the RRAM array with many random challenges in a secure environment. The resulting Challenge-Response Pairs (CRPs) are obtained as a "signature" for the node itself and are stored in a secure database.

Authentication (Field Verification): Central authority calls challenge C and a random Nonce. Node computes R physically. Node calculates a one-way Hash (R || Nonce) as part to deter replay attacks. The hash is also verified with its trusted database by authority. The verification condition accepts a small error δ to control aging and noise:

$$HD(R_{measured}, R_{enrolled}) < \delta \tag{10}$$

B. *Use Case for Fraud Mitigation*

Affixing the cryptographic identity securely to the physical silicon will allow for:

Hardware Provenance: This will help to ensure that counterfeit parts cannot be inserted into the supply chain

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 5, Issue – 1, June 2026
E – ISSN – 2583-7559

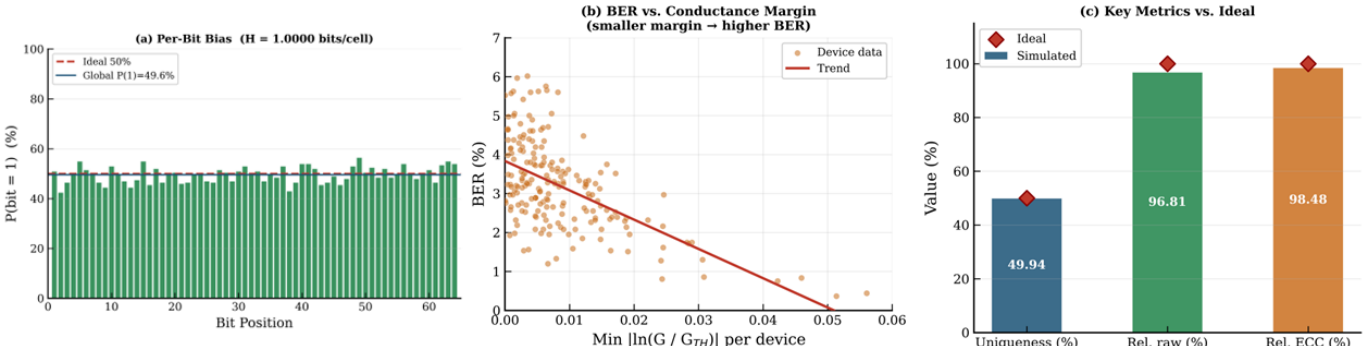


Fig. 3. Monte Carlo simulation results (continued). (200 devices, 64-bit response, $\sigma_{ln} = 0.4, \sigma_{read} = 0.04$). (a) Per-bit-position bias, $P(R = 1) = 0.4959$. (b) BER vs. conductance margin, cells closer to G_{TH} show higher BER, physically motivating fuzzy extraction. (c) Summary of key metrics vs. ideal.

Rogue Base Station Defense: A clone device will be unable to generate the correct R value regardless of whether it is in possession of the correct software key. This is due to the lack of specific vacancy distribution for the authorized silicon device.

Simbox (Rogue VoIP Gateway) Detection: Hardware identity binding during gateway enrollment ensures only silicon with a verified physical fingerprint is admitted into the routing infrastructure. A Simbox, even if loaded with legitimate routing software, cannot reproduce the RRAM conductance fingerprint of an authorized gateway.

SIM Provisioning Server Authentication: RRAM-PUF identity anchoring at provisioning nodes reduces risk of mass credential replication. Since server authentication cannot be bypassed without physically cloning the silicon, with clone probability 5.42×10^{-20} for a 64-bit PUF, unauthorized SIM mass-generation is computationally and physically infeasible.

IMSI Catcher Defense: Because the PUF response is derived from atomic-level oxygen-vacancy positions, a rogue base station that intercepts and replicates the challenge stream cannot produce a valid response without possessing the exact physical device, mitigates IMSI-catcher insertion attacks.

VI. Hardware Security Advantages, Latency and Hardware Overhead

A. Non-Volatility

The resistance state of RRAM does not depend on power: $G_i(t) \approx G_i(0)$. In contrast to SRAM-based PUFs that depend on meta-stable power-up states, RRAM enables "instant-on" authentication. The filament state is thermodynamically stable over time (usually about 10 years at 85ºC).

Arrhenius modelling (Fig. 2(a)) with activation energy E_a = 1.2 eV confirms conductance drift of less than 5% across the operating temperature range of −23°C to 85°C, well within the tolerance band of the fuzzy extractor.

B. Resistance to Cloning

The security of this technique hinges on the complexity of an Atomic-Level clone. For a physical clone to develop, an attacker would need to model the exact location of oxygen vacancies in the oxide. Because ion hopping happens randomly [18], [19], the chance of two independent devices possessing identical filament shapes (P_{clone}) is almost zero. Moreover, invasive probing (e.g. FIB) typically shifts the amount of oxygen concentration, thereby destroying the key ("Tamper Evidence").

For the proposed 64-bit RRAM-PUF, $P_{clone} = 0.5^{64} = 5.42e^{-20}$, quantitatively confirming that physical duplication is infeasible even against adversaries with advanced fabrication capabilities.

C. Resilience to Machine Learning Attacks

Linear summation PUFs are theoretically vulnerable to modeling attacks if the attacker harvests a large enough number of CRPs [22]. This is resolved according to the architecture by using a non-linear masking layer (e.g., a hash or XOR network) at the output, causing the output to hide the linear relationship between C and I_j.

D. Latency and Hardware Overhead

Authentication time is given by:

$$T_{auth} = T_{read} + T_{compare} \quad (11)$$

Because the parallel multiplication vector–matrix $(V \times G)$ happens in the analog domain, T_{read} is essentially constant independent of vector length [3]. This accumulation occurs in accordance with the rate of electric signal propagation. Energy consumption is:

$$E = V_{read} \cdot I_{total} \cdot T_{read} \quad (12)$$

Since the engine operates in the femto-Joule/bit regime, the high-resistance state (HRS) and low read voltages are applied, thus enabling high efficiencies over CPU-heavy cryptographic operations.

Simulation-derived estimates yield T_{auth} = 10 ns and E = 768 fJ for a 64-bit authentication operation (12 fJ/bit), representing improvements of several orders of magnitude over conventional software-key cryptographic operations (typically in the μJ range).

VII. Threat Model and Practical Considerations: Stability and Fuzzy Extractors

The system protects against:

Physical Cloning: Resilient to cloning even with inspection from sophisticated techniques such as Atomic Force Microscopy or Focused Ion Beam.

Software Emulation: Software cannot replicate the original analog response characteristics of the hardware device as copying of the underlying firmware is never enough.

Man-in-the-Middle Replays: Avoided using dynamic Nonces in the hashing stage. It adopts a Secure Enrollment Phase whereby the initial characterization is taken before the device leaves the trusted supply chain.

A comparison between the proposed RRAM-PUF framework and conventional software-based key storage approaches across security and performance parameters such as key storage, cloning, latency etc. is detailed in Table II.

TABLE II. Comparative Perspective

Parameter	Software Key Storage	RRAM-PUF (Proposed)
Key Storage	Digital memory (Vulnerable)	Physics-derived (Secure)
Cloning	Possible (Digital Copy)	Impossible (Atomic random)
Latency	Multi-cycle (CPU Arithmetic)	Single cycle (In-Memory Physics)
Tamper Evidence	Low	High (Probing alters vacancies)
Auth. Energy (64-bit)	μJ /op (CPU)	768 fJ (analog in-memory)

Ideally G_i value would remain constant, however in practicality upon taking Arrhenius equation into consideration, it can vary with temperature

$$G_i(T) = G_i(0) \cdot \exp\left(-\frac{E_a}{k_B T}\right) \quad (13)$$

Fuzzy Extractors are deployed to overcome bit flips that are caused by temperature or read noise [23]. It is a "Secure Sketch" or "Helper Data" created as a result of enrollment. This data (W) enables the system to map a noisy reading R' back to R. This helps to ensure precise key regeneration without revealing any information about the secret.

The simulated raw BER of 3.19% confirms that a fuzzy extractor in addition to being theoretically desirable is operationally necessary. When error correction is not executed, on average approximately 2 bits in a 64-bit response would flip per authentication event. A BCH (63, 36, t=5) code reduces the post-correction failure probability to less than 1.55%. Thus, it is able to yield a post-ECC reliability of 98.48%.

VIII. Conclusion

We presented an RRAM-based physically unclonable authentication engine for secure telecom infrastructure. The stochastic conductance variation is inherent to each RRAM device due to the thermodynamic randomness of oxygen vacancy filament formation and hence is modeled as an entropy source. A theoretical and simulation-based framework has been introduced for future implementation. A mathematical formulation for uniqueness, reliability and randomness validates the architecture without reliance on stored cryptographic keys. A Monte Carlo simulation across 200 device instances validated the theoretical framework with uniqueness of 49.94%, raw reliability of 96.81% (BER = 3.19%), post-ECC reliability of 98.48% using BCH(63,36,t=5), and entropy of 1 bits/cell which are consistent with published RRAM-PUF benchmarks. Incorporating fuzzy extractor for error correction further improves the response stability and enhance reliability, clone resistant Hardware Root of Trust. The proposed framework provides solution to critical fraud in telecom networks ensuring only authorized participation with verified physical provenance carries subscriber traffic.

Acknowledgment

The authors are grateful to Multidisciplinary Research & Innovation Center, National Forensic Sciences University, Goa Campus, and School of Cyber Security and Digital Forensics, National Forensic Sciences University, Gandhinagar for the opportunity to conduct this research.

References

[1] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

[2] H.-S. P. H.-S. P. H.-S. P. Wong *et al.*, "Metal–Oxide RRAM," *Proc. IEEE*, vol. 100, no. 6, pp. 1951–1970, Jun. 2012, doi: 10.1109/JPROC.2012.2190369.

[3] A. Chen, "Comprehensive assessment of RRAM-based PUF for hardware security applications," in *2015 IEEE International Electron Devices Meeting (IEDM)*, IEEE, Dec. 2015, pp. 10.7.1-10.7.4. doi: 10.1109/IEDM.2015.7409672.

[4] V. Pandey, A. Adiba, T. Ahmad, P. Nehla, and S. Munjal, "Forming-free bipolar resistive switching characteristics in Al/Mn3O4/FTO RRAM device," *J. Phys. Chem. Solids*, vol. 165, p. 110689, Jun. 2022, doi: 10.1016/j.jpcs.2022.110689.

[5] S. Shivaram, S. K. S. Babu, D. R. Paul, and A. Ashok, "Engineering

TiO_2 memristors: A material-centric review," *J. Mater. Res.*, vol. 40, no. 10, pp. 1449–1479, May 2025, doi: 10.1557/s43578-025-01600-z.

[6] O. P. Das and S. K. Pandey, "Exploring the Physical Properties Related to Resistive Switching Events in HfO 2 -Based RRAM Devices with an Analytical Framework," *ACS Appl. Electron. Mater.*, vol. 5, no. 1, pp. 327–334, Jan. 2023, doi: 10.1021/acsaelm.2c01350.

[7] D. Chaudhary, S. Munjal, N. Khare, and V. D. Vankar, "Bipolar resistive switching and nonvolatile memory effect in poly (3-hexylthiophene) –carbon nanotube composite films," *Carbon N. Y.*, vol. 130, pp. 553–558, Apr. 2018, doi: 10.1016/j.carbon.2018.01.058.

[8] K. Rudrapal, M. Biswas, B. Jana, V. Adyam, and A. R. Chaudhuri, "Tuning resistive switching properties of WO 3− x -memristors by oxygen vacancy engineering for neuromorphic and memory storage applications," *J. Phys. D. Appl. Phys.*, vol. 56, no. 20, p. 205302, May 2023, doi: 10.1088/1361-6463/acc258.

[9] M. T. A. S. Shaikh *et al.*, "Multilevel Reset Dependent Set of a Biodegradable Memristor with Physically Transient," *Adv. Sci.*, vol. 11, no. 4, Jan. 2024, doi: 10.1002/advs.202306206.

[10] V. Pandey, P. Nehla, and S. Munjal, "Controlled Self Compliance Filamentary Memory Behavior in Al/NiFe2O4/FTO Resistive Switching Device," *Proc. Natl. Acad. Sci. India Sect. A Phys. Sci.*, vol. 93, no. 3, pp. 451–457, Sep. 2023, doi: 10.1007/s40010-023-00842-y.

[11] Anita and A. Kumar, "Electric Field Modulated SET and RESET Resistive Switching Process in Hafnia Zirconia Oxide," *Phys. status solidi*, vol. 223, no. 15, Aug. 2026, doi: 10.1002/pssa.70446.

[12] J. Ryu, K. Park, D. P. Sahu, and T.-S. Yoon, "Forming-Free, Low-Voltage, and High-Speed Resistive Switching in Ag/Oxygen-Deficient Vanadium Oxide(VO x)/Pt Device through Two-Step Resistance Change by Ag Filament Formation," *ACS Appl. Mater. Interfaces*, vol. 16, no. 20, pp. 26450–26459, May 2024, doi: 10.1021/acsami.4c04874.

[13] S. Munjal and N. Khare, "Compliance current controlled volatile and nonvolatile memory in Ag/CoFe 2 O 4 /Pt resistive switching device," *Nanotechnology*, vol. 32, no. 18, p. 185204, Apr. 2021, doi: 10.1088/1361-6528/abdd5f.

[14] M. Hellenbrand *et al.*, "Thin film design of amorphous hafnium oxide nanocomposites enabling strong interfacial resistive switching uniformity," *Sci. Adv.*, vol. 9, no. 25, Jun. 2023, doi: 10.1126/sciadv.adg1946.

[15] J. Zhao *et al.*, "An electronic synapse memristor device with conductance linearity using quantized conduction for neuroinspired computing," *J. Mater. Chem. C*, vol. 7, no. 5, pp. 1298–1306, 2019, doi: 10.1039/C8TC04395G.

[16] S. Munjal and N. Khare, "Advances in resistive switching based memory devices," *J. Phys. D. Appl. Phys.*, vol. 52, no. 43, p. 433002, Oct. 2019, doi: 10.1088/1361-6463/ab2e9e.

[17] A. Adiba, V. Pandey, T. Ahmad, P. Nehla, and S. Munjal, "Multilevel resistive switching with negative differential resistance in Al/NiO/ZnFe2O4/ITO ReRAM device," *Phys. B Condens. Matter*, vol. 654, p. 414742, Apr. 2023, doi: 10.1016/j.physb.2023.414742.

[18] M. Zhao *et al.*, "Crossbar-Level Retention Characterization in Analog RRAM Array-Based Computation-in-Memory System," *IEEE Trans. Electron Devices*, vol. 68, no. 8, pp. 3813–3818, Aug. 2021, doi: 10.1109/TED.2021.3089561.

[19] D. Ielmini, "Modeling the Universal Set/Reset Characteristics of Bipolar RRAM by Field- and Temperature-Driven Filament Growth," *IEEE Trans. Electron Devices*, vol. 58, no. 12, pp. 4309–4317, Dec. 2011, doi: 10.1109/TED.2011.2167513.

[20] H. Panchal, N. K. Chaudhary, and S. Munjal, "A Mini Review on—Physically Unclonable Functions: The Hardware Security Primitives," 2024, pp. 305–316. doi: 10.1007/978-981-99-5091-1_22.

[21] A. Maiti, V. Gunreddy, and P. Schaumont, "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," in *Embedded Systems Design with FPGAs*, New York, NY: Springer New York, 2013, pp. 245–267. doi: 10.1007/978-1-4614-1362-2_11.

[22] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 237–249.

[23] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008, doi: 10.1137/060651380.