An Evaluation of LM35 Temperature Sensors as Physical Unclonable Functions

Selma Brimah*, Shekoufeh Neisarian*†★, Elif Bilge Kavun†‡★,
Stefan Katzenbeisser*, Tolga Arul*§, Nikolaos Athanasios Anagnostopoulos*
*Universität Passau – Emails: {brimah01, neisar01, katzen07, arul01, anagno02}@ads.uni-passau.de
†Barkhausen Institute – Emails: {shekoufeh.neisarian, elif.kavun}@barkhauseninstitut.org
‡Dresden University of Technology – Email: elif_bilge.kavun@tu-dresden.de
§Technical University of Darmstadt – Email: arul@rbg.informatik.tu-darmstadt.de

2025 IEEE Zooming Innovation in Consumer Technologies Conference (ZINC) | 979-8-3315-1152-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/ZINC65316.2025.11103559

***Abstract*—This paper explores the feasibility of employing LM35 temperature sensors as Physical Unclonable Functions (PUFs) for secure identification and cryptographic applications. PUFs exploit inherent hardware variations to generate unique and non-replicable identifiers, offering a novel alternative to traditional cryptographic keys. Five LM35 sensors were tested in controlled indoor and dynamic outdoor environments to assess their uniqueness, robustness, and stability. The sensors' voltage outputs, influenced by manufacturing tolerances and intrinsic variations, were analyzed for potential use as cryptographic tokens. The results demonstrated that while the different sensors exhibited some response variation, their outputs lacked the consistency and distinctiveness required for robust PUF applications. Controlled conditions yielded more stable responses, whereas outdoor environments introduced variability that compromised reliability. These findings underscore the limitations of LM35 sensors as PUFs, suggesting the need for dedicated security modules or hybrid approaches to achieve practical security solutions. Our study highlights challenges in sensor-based PUFs and offers insights for future research.**

***Index Terms*—Physical Unclonable Functions (PUFs), LM35, temperature sensors, stability, uniqueness**

I. Introduction

Physical Unclonable Functions (PUFs) offer a hardware-based method for secure identification, leveraging minor unique variations to generate secure identifiers. Such minor variations are inherent in physical devices and they do not affect their main functionality. Unlike conventional cryptographic keys, which are susceptible to replication and manipulation, PUFs capitalize on intrinsic hardware properties that are challenging to replicate on another device and produce cryptographic tokens that require only ephemeral storage. Recent studies have explored various hardware sources as potential PUFs, yet limited research has investigated the suitability of sensor-based PUFs, particularly in resource-constrained environments like the Internet of Things (IoT) [1], [2].

This work has been partially funded by the German Research Foundation – Deutsche Forschungsgemeinschaft (DFG), under Projects 440182124: "PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories", 439892735: "NANOSEC: Tamper-Evident PUFs Based on Nanostructures for Secure and Robust Hardware Security Primitives", and the Young Scientist Project "Chaos-Based Secure Communication" of the Priority Program – SchwerPunktProgramme (SPP) 2253: "Nano Security: From Nano-Electronics to Secure Systems".

★S. Neisarian and E. B. Kavun were with the University of Passau at the time of writing.

Drawing inspiration from a recent work examining the capability of Pt100 and Pt1000 temperature sensors to act as PUFs [3], this work explores the feasibility of using LM35 temperature sensors as PUFs. The LM35 sensor, known for its low cost, accuracy, and linear voltage-temperature relationship, may exhibit response variations due to inherent manufacturing inconsistencies. These variations could potentially serve as cryptographic tokens, leading even to the production of potentially unique identifiers and keys. To this end, our research evaluates whether these sensors produce unique and stable outputs under stable ambient temperatures and assesses their potential to serve as secure, low-cost identification mechanisms.

II. Related Work

Physical Unclonable Functions (PUFs) have become increasingly relevant in hardware security, leveraging intrinsic manufacturing variations to create device-specific identifiers. Early contributions by Gassend et al. [4], Guajardo et al. [5], and Holcomb et al. [6] established the foundations first of silicon-based and then of silicon-memory-based PUFs, while Lee et al. [7] introduced error correction to enhance stability.

Recent work has extended PUF concepts to sensor-based systems. Ma et al. [8] proposed a universal sensor PUF integrating voltage sensitivity to enhance entropy. Their approach highlighted the role of unreliable response bits and environmental influences such as voltage and temperature in generating unique outputs. Similarly, Rosenfeld et al. [9] presented "sensor PUFs" to combat spoofing by securely linking sensing and authentication using continuous response processing. Additionally, Arjona et al. [10] proposed composite architectures that integrate PUFs and biometric features to improve the security of sensor nodes and mitigate the impact of environmental noise.

Research by Hristov et al. [11], Stavrinides et al. [12], and Fukushima et al. [13] explored photodiode- and accelerometer/gyroscope-based PUFs, confirming their potential in widely available IoT devices. Moreover, Lee et al. [14] examined a PUF based on the use of resistor-capacitor couples, in the context of resource-constrained IoT devices. In temperature-based implementations, Labrado et al. [15] investigated Positive-Temperature-Coefficient (PTC) thermistor-

based PUFs, showing reliability in standard conditions, though performance declined under very low temperatures, and the proposed PUF may be vulnerable to cloning attacks. Finally, Bahoum et al. [3] investigated resistance variability in PT100 and PT1000 temperature sensors, identifying PT100 as a more promising candidate for PUF realisation due to its distinctive behaviour under thermal fluctuations.

These studies collectively highlight the trend towards exploiting intrinsic device properties – such as electrical, optical, or thermal – to design lightweight, resilient, and efficient PUFs suited for securing next-generation IoT systems. However, challenges remain towards realising temperature-sensor-based PUFs for real-world deployment. Apart from cloning attacks, and the effects of aging and environmental factors on sensor-based PUFs in general, the characteristic properties of temperature sensors may inherently exhibit so much instability that their utilisation as PUFs is rather infeasible.

Nevertheless, although silicon PUFs dominate the literature, the potential of a number of different sensors to serve as PUFs has been explored in the relevant literature. Thus, the evaluation of the potential of LM35 temperature sensors to work as PUFs represents a novel and promising direction that has not yet been examined in the existing related work. Our study aims to address this gap in the literature, and in this way provide further insights into the capability of temperature sensors to act as security primitives that could be utilised to allow for cryptographic applications in the framework of embedded systems and the IoT.

III. Methodology

This work examines the responses of five IDUINO LM35 temperature sensor (SE039) board[1] instances to test their characteristic behaviour in three different environments: inside a climate chamber with fully controlled temperature, under rather controlled indoor conditions, as well as under rather uncontrolled outdoor conditions. Each LM35 sensor board was connected to an Analog-to-Digital Converter (ADC) interfaced with a Raspberry Pi 3 Model B+ to capture and record its voltage outputs relative to ambient temperature in order to identify the different patterns produced under different (rather stable) ambient temperatures. In the indoor setting, a heater was used to keep the temperature rather stable, allowing for consistent measurements. In the uncontrolled outdoor setup, natural temperature variations occurred over time.

A. Data Collection

To ensure a reliable assessment, the experiment was conducted using a total of five LM35 temperature sensors. Each sensor underwent five separate measurement cycles across three environments: indoor, outdoor, and climate chamber, at a different somewhat stable temperature in each environment. These repeated cycles at different temperatures and environments were designed to evaluate the consistency and uniqueness of sensor responses over time and under varying temperature conditions. This structured approach helped establish a comparative basis for analyzing sensor performance under different temperature values and environmental conditions. Sensor data were collected at regular intervals during each measurement cycle. The analog voltage outputs from the LM35 sensors were converted to temperature values using their linear voltage-to-temperature relationship. These temperature readings were processed and analyzed to identify response patterns and deviations across sensors and conditions.

The average indoor temperature was approximately 24°C, while the outdoor environment fluctuated around the region of 5°C. The climate chamber was maintained at a stable 23°C with controlled humidity, providing a benchmark for evaluating sensor performance in highly regulated conditions. For each environment, data from all sensors and cycles were averaged to facilitate their comparative analysis. The study focused on two key metrics:

- **Uniqueness:** The degree to which each sensor exhibited distinct voltage responses in comparison to the other sensors under similar environmental conditions.
- **Robustness:** The consistency of each sensor's response under the same ambient temperature and test scenario.

IV. Results and Analysis

Box plots were constructed to represent the temperature measurement distribution of each sensor in each environment, effectively capturing the range, median, and outlier behaviours of the sensors. These visualizations facilitated a detailed comparison of sensor performance under varying temperature values and environmental conditions, as illustrated in Figure 1, Figure 2, and Figure 3, for the rather controlled indoor environment, the rather uncontrolled outdoor conditions, and the fully controlled climate chamber, respectively.

In the indoor environment, as shown in Figure 1, the temperature measurement distributions were relatively stable, with medians clustering around 24°C for sensor instances #1, #2, and #3. Sensor instance #4 displayed a slightly higher median temperature, and sensor instance #5 exhibited an even higher median temperature (at around 25°C) compared to all the other sensor instances. Notably, the readings of sensor instance #1 covered a larger range than all the other sensor instances, while sensor instances #2, and #5 had rather prominent outliers, with both cases potentially reflecting inconsistencies in the behaviour of the relevant sensor instances, even under somewhat controlled conditions.

In contrast, the outdoor environment, in general, led to greater variability in temperature measurement distributions, as evidenced by wider boxes and longer whiskers (shown in Figure 2). The median temperature values for sensor instances #1, #2, and #3 clustered at around 5°C, reflecting the colder outdoor conditions. Again, sensor instance #4 displayed a slightly higher median temperature, and sensor instance #5 exhibited an even higher median temperature (at around 6°C) compared to all the other sensor instances. All sensor instances exhibited a rather broad Inter-Quartile Range (IQR) as well as a number of outliers, indicating greater variability

[1]https://www.openplatform.cc/index.php/home/index/details/apiid/191

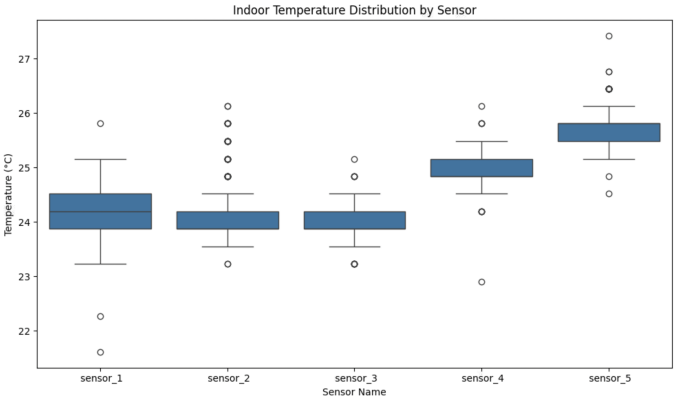

Fig. 1. Box plots demonstrating the variation in the distribution of the indoor temperature measurements of each sensor.

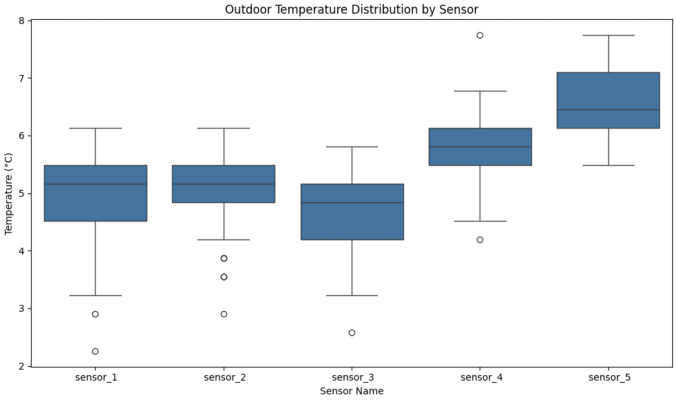

Fig. 2. Box plots demonstrating the variation in the distribution of the outdoor temperature measurements of each sensor.

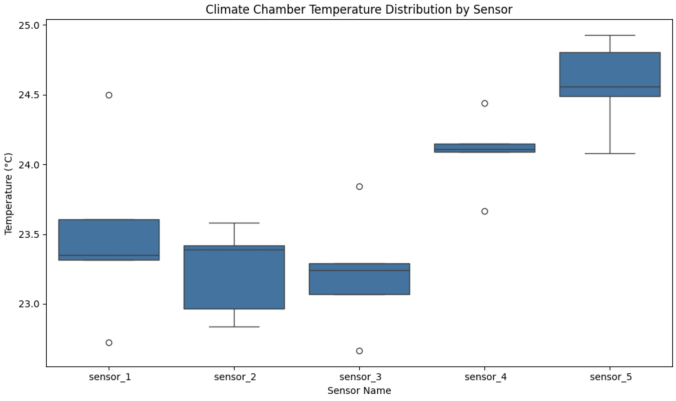

Fig. 3. Box plots demonstrating the variation in the distribution of the climate chamber temperature measurements of each sensor.

in their readings, underscoring the influence of dynamic and fluctuating temperature conditions on sensor performance.

Regarding the climate chamber measurements, where sensors were evaluated under tightly controlled temperature conditions (23°C), the readings reflected distributions within smaller ranges in comparison to the outdoor measurements and rather similar to the indoor setup, as demonstrated in Figure 3.

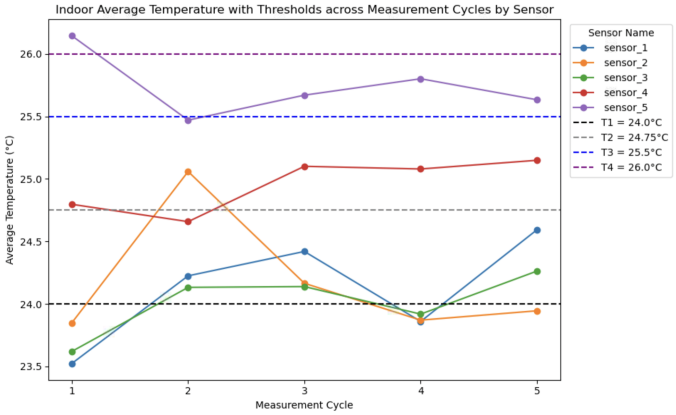

Fig. 4. Line plots for the average indoor temperature measurement for each sensor instance at each measurement cycle, along with the relevant thresholds.

However, most sensor instances exhibited single outliers that deviated by more than 0.5°C from the main distribution. Once again, sensor instance #4 displayed a slightly higher median temperature (at around 24°C), and sensor instance #5 exhibited an even higher median temperature (at around 24.5°C) and a broader IQR compared to all the other sensor instances.

A. *Threshold-Based Evaluation*

The indoor temperature readings from the examined sensor instances were analyzed using four binary thresholds, T1 = 24.0°C, T2 = 24.75°C, T3 = 25.5°C, and T4 = 26.0°C. The thresholds served to categorize the temperature responses of each sensor into binary outputs. For each threshold and sensor instance, a binary string was formed based on whether that sensor instance's temperature readings were exceeding the relevant threshold or not. For example, if the first measurement cycle's temperature reading of a particular sensor instance was exceeding the relevant threshold, then the first bit of the corresponding bit string for that sensor instance and threshold was set to 1, otherwise to 0. This process was repeated for the five measurement cycles of each of the five sensor instances and the four thresholds, resulting in a binary threshold table, Table I.

In this way, binary strings were generated for each sensor across all measurement cycles, reflecting its behaviour relative to the predefined thresholds. These binary representations facilitated the identification of unique response patterns for individual sensors. Thus, Table I presents the binary threshold encoding derived from the line plot shown in Figure 4, which shows the average temperature for each sensor instance at each measurement cycle for the indoor setup.

For the outdoor temperature readings, thresholds were adjusted to account for the lower average temperatures, with T1 = 4.5°C, T2 = 5.0°C, T3 = 5.5°C, and T4 = 6.0°C. The same binary encoding approach as before was applied. Binary strings were generated for each sensor, capturing its response to the dynamic temperature fluctuations of the outdoor setup. To this end, Table II shows the binary threshold encoding derived from the line plots illustrated in Figure 5, which

TABLE I
BINARY THRESHOLD ENCODING FOR THE INDOOR TEMPERATURE DATA

	T1	*T2*	*T3*	*T4*
Sensor 1	01101	00000	00000	00000
Sensor 2	01100	01000	00000	00000
Sensor 3	01101	00000	00000	00000
Sensor 4	11111	10111	00000	00000
Sensor 5	11111	11111	10111	10000

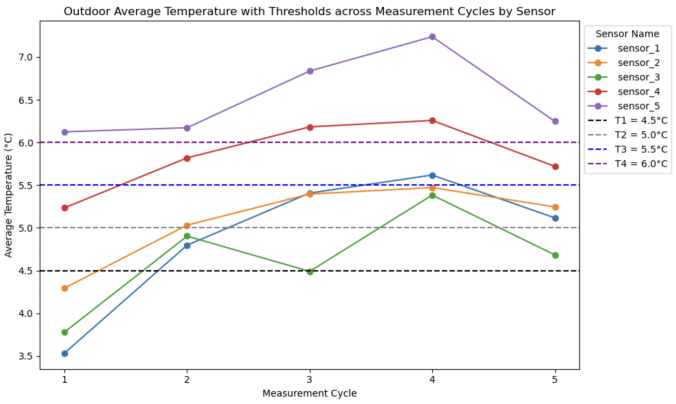

Fig. 5. Line plots for the average outdoor temperature measurement for each sensor instance at each measurement cycle, along with the relevant thresholds.

TABLE II
BINARY THRESHOLD ENCODING FOR
THE OUTDOOR TEMPERATURE DATA

	T1	*T2*	*T3*	*T4*
Sensor 1	01111	00111	00010	00000
Sensor 2	01111	01111	00000	00000
Sensor 3	01011	00010	00000	00000
Sensor 4	11111	11111	01111	00110
Sensor 5	11111	11111	11111	11111

shows the average temperature for each sensor instance at each measurement cycle for the outdoor environment.

For the climate chamber temperature readings, the thresholds were adjusted to T1 = 22.8°C, T2 = 23.5°C, T3 = 24°C, and T4 = 24.5°C, to account for lower average temperatures than the indoor setup. Binary strings were generated for each sensor for all measurement cycles using the same binary encoding approach as before, resulting in Table III. This table presents the binary threshold encoding derived from the line plots shown in Figure 6, which demonstrates the average temperature for each sensor instance at each measurement cycle for the climate chamber environment.

B. Measurement-Level Binary Encoding

To evaluate sensor behaviour more precisely, a measurement-level binary encoding approach was also applied. Each average temperature measurement per measurement cycle was compared against five environment-specific thresholds, resulting in a 5-bit binary string. For example, if the average temperature measurement for a particular

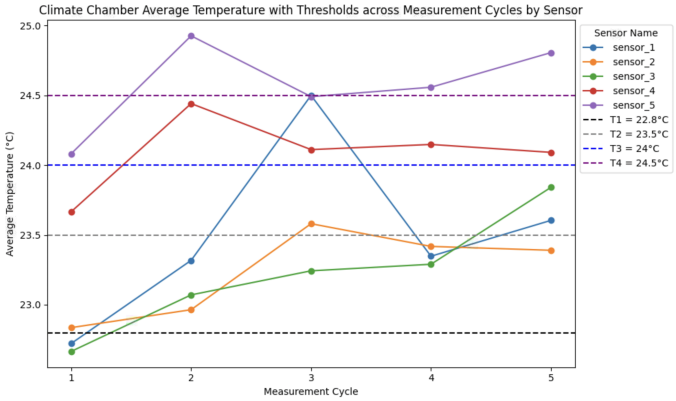

Fig. 6. Line plots for the average climate chamber temperature measurement for each sensor instance at each measurement cycle, along with the relevant thresholds.

TABLE III
BINARY THRESHOLD ENCODING FOR
THE CLIMATE CHAMBER TEMPERATURE DATA

	T1	*T2*	*T3*	*T4*
Sensor 1	01111	00101	00100	00100
Sensor 2	11111	00100	00000	00000
Sensor 3	01111	00001	00000	00000
Sensor 4	11111	11111	01111	00000
Sensor 5	11111	11111	11111	01011

measurement cycle of a specific sensor instance exceeded the relevant first threshold value, then the first bit of the corresponding bit string was set to 1, otherwise to 0. This process was repeated for all the relevant thresholds and the five measurement cycles of each sensor instance for all the experimental setups employed in this study.

The relevant threshold values for each experimental setup were defined as follows:

- **Indoor Environment:** 24.0°C, 24.5°C, 25.0°C, 25.5°C, 26.0°C
- **Outdoor Environment:** 4.0°C, 4.5°C, 5.0°C, 5.5°C, 6.0°C
- **Climate Chamber:** 23.0°C, 23.5°C, 24.0°C, 24.5°C, 25.0°C

The aforementioned process resulted in the generation of binary strings in a similar manner as the process detailed in the previous subsection. Hence, the relevant bit strings for the measurement-level binary encoding explained in this subsection can be found in Table IV, Table V, and Table VI, for the rather controlled indoor environment, the rather uncontrolled outdoor conditions, and the fully controlled climate chamber, respectively.

C. Discussion

As Figures 1, 2 and 3 reveal, the examined IDUINO LM35 temperature sensor (SE039) board instances exhibit, for all the environments tested, insufficient uniqueness, as their readings may significantly overlap, and at the same time, also an inadequate degree of robustness, as the readings of a particular

TABLE IV
MEASUREMENT-LEVEL BINARY ENCODING FOR THE INDOOR ENVIRONMENT

	M1	M2	M3	M4	M5
Sensor 1	00000	10000	10000	00000	11000
Sensor 2	00000	11100	10000	00000	00000
Sensor 3	00000	10000	10000	00000	10000
Sensor 4	11000	11000	11100	11100	11100
Sensor 5	11111	11100	11110	11110	11110

TABLE V
MEASUREMENT-LEVEL BINARY ENCODING FOR THE OUTDOOR ENVIRONMENT

	M1	M2	M3	M4	M5
Sensor 1	00000	11000	11100	11110	11100
Sensor 2	10000	11100	11100	11100	11100
Sensor 3	00000	11000	10000	11100	11000
Sensor 4	11100	11110	11111	11111	11110
Sensor 5	11111	11111	11111	11111	11111

TABLE VI
MEASUREMENT-LEVEL BINARY ENCODING FOR THE CLIMATE CHAMBER

	M1	M2	M3	M4	M5
Sensor 1	00000	10000	11110	10000	11000
Sensor 2	00000	00000	11000	10000	10000
Sensor 3	00000	10000	10000	10000	11000
Sensor 4	11000	11100	11100	11100	11100
Sensor 5	11100	11110	11100	11110	11110

sensor at extremely stable ambient temperature conditions (within a climate chamber, as demonstrated in Figure 3) may vary by up to 1°C from each other. While one might have expected that the degree of uniqueness in the readings of different sensors of the same type would at best be rather limited, the concurrent instability of the measurements of the same sensor at stable ambient temperature is rather counter-intuitive. Moreover, while in Figures 1, 2 and 3 the readings of sensor instances #4 and #5 appear to be somewhat distinct from those of sensors #1, #2, and #3, Figures 4, 5 and 6 clearly show that this is not truly the case, as the average temperature reading per measurement cycle of different sensor instances are extremely close, even in the case of extremely stable ambient temperature conditions (within a climate chamber, as demonstrated in Figure 6), where the average temperature reading of sensor instance #1 for measurement cycle 3 almost overlaps with that of sensor instance #5.

These findings are further supported by both approaches of binary encoding. In all cases (as demonstrated in Tables I, II and III for the binary threshold encoding approach, and in Tables IV, V and VI for the measurement-level binary encoding approach), the relevant binary strings clearly indicate a lack of robustness, as the bit strings of the same sensor may differ by any number of bits. More specifically, responses corresponding to measurements of the same sensor may differ by 2-3 bits (≈50% difference) or by all their 5 bits (100% difference), even in the case of extremely stable ambient temperature conditions (within a climate chamber, as indicated in Tables III and VI). Additionally, it is obvious that the responses of different sensors may also completely match each other in all the three different environments examined, indicating a complete lack of uniqueness.

Thus, the tested LM35 sensors, in general, exhibit insufficient robustness and uniqueness to support their utilisation as reliable PUFs. The relevant minor manufacturing variations do not lead to unique readings in any of the settings examined and the sensor readings are unstable even under extremely stable ambient temperature conditions within a climate chamber.

V. CONCLUSION

This work examined the feasibility of using LM35 temperature sensors as PUFs. Five IDUINO LM35 temperature sensor (SE039) boards were tested in three different environments: inside a climate chamber with fully controlled temperature, under rather controlled indoor conditions, as well as under rather uncontrolled outdoor conditions. In each environment, sensor data were collected at regular intervals within five measurement cycles. The analog voltage outputs from the LM35 sensors were converted to temperature values using their linear voltage-to-temperature relationship. These temperature readings were then processed and analysed in terms of their robustness and uniqueness.

As the results of our analysis reveal, the examined LM35 temperature sensors do not exhibit the unique and robust characteristics required for effective use as PUFs in cryptographic applications. While sensor-based PUFs have the potential to be used for the creation of secure, low-cost cryptographic schemes and identification mechanisms, the inherent characteristics of LM35 sensors do not appear to provide adequate stability or distinctiveness in order to serve as PUFs. Consequently, alternative sensors with higher intrinsic uniqueness and variability, dedicated security modules, or hybrid approaches, may be necessary to achieve the realisation of reliable PUFs.

Future work should explore alternative technologies offering higher robustness and uniqueness. In particular, other analog temperature sensors, such as TMP35 and Negative-Temperature-Coefficient (NTC) thermistors, should also be investigated as potential PUFs. Furthermore, composite PUF architectures, combining multiple sensor types, other complementary encryption mechanisms to address the limitations of environmental sensors, and/or machine learning techniques for entropy extraction, represent valuable paths to explore in order to potentially enhance security and performance. Further research is also required in the direction of creating appropriate lightweight protocol designs for IoT environments to enable the scalable deployment of sensor-based security mechanisms in practice.

ACKNOWLEDGMENT

Parts of this work have been included in the master's thesis of Selma Brimah [16].

REFERENCES

[1] B. M. S. Bahar Talukder, F. Ferdaus, and M. T. Rahman, "Memory-based PUFs are vulnerable as well: A non-invasive attack against SRAM PUFs," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4035–4049, 2021. [Online]. Available: https://doi.org/10.1109/TIFS.2021.3101045

[2] A. Babaei and G. Schiele, "Physical unclonable functions in the internet of things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, 2019. [Online]. Available: https://doi.org/10.3390/s19143208

[3] E. M. Bahoum, N. Mexis, S. Katzenbeisser, T. Arul, and N. A. Anagnostopoulos, "Testing temperature-dependent resistors as potential physical unclonable functions," in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*. IEEE, 2024, pp. 407–413. [Online]. Available: https://doi.org/10.1109/WF-IoT62078.2024.10811170

[4] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02. Association for Computing Machinery, 2002, pp. 148–160. [Online]. Available: https://doi.org/10.1145/586110.586132

[5] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Cryptographic Hardware and Embedded Systems – CHES 2007*, ser. Lecture Notes in Computer Science (LNCS), P. Paillier and I. Verbauwhede, Eds., vol. 4727. Springer, 2007, pp. 63–80. [Online]. Available: https://doi.org/10.1007/978-3-540-74735-2_5

[6] D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proceedings of the Conference on RFID Security 2007*, 2007. [Online]. Available: http://www.rfidsec07.etsit.uma.es/slides/papers/paper-12.pdf

[7] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Digest of Technical Papers of the 2004 Symposium on VLSI Circuits (VLSIC)*. IEEE, 2004, pp. 176–179. [Online]. Available: https://doi.org/10.1109/VLSIC.2004.1346548

[8] H. Ma, Y. Gao, O. Kavehei, and D. C. Ranasinghe, "A PUF sensor: Securing physical measurements," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 648–653. [Online]. Available: https://doi.org/10.1109/PERCOMW.2017.7917639

[9] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2010, pp. 112–117. [Online]. Available: https://doi.org/10.1109/HST.2010.5513103

[10] R. Arjona, M. Á. Prada-Delgado, J. Arcenegui, and I. Baturone, "A PUF- and biometric-based lightweight hardware solution to increase security at sensor nodes," *Sensors*, vol. 18, no. 8, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/8/2429

[11] E. Hristov, R. Picos, C. de Benito, S. G. Stavrinides, T. Arul, N. A. Anagnostopoulos, and M. M. Al Chawa, "Implementation of a physically unclonable function using LEDs and LDRs," in *2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2023, pp. 1–4. [Online]. Available: https://doi.org/10.1109/MOCAST57943.2023.10176623

[12] S. G. Stavrinides, L. Bush-Espinosa, C. de Benito, N. A. Anagnostopoulos, T. Arul, S. Katzenbeisser, C. Tjortjis, M. M. Al Chawa, and R. Picos, "Exploiting optical nonlinear temporal coupling for implementing physical unclonable functions," in *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*. IEEE, 2023, pp. 1–5. [Online]. Available: https://doi.org/10.1109/WF-IoT58464.2023.10539389

[13] K. Fukushima, S. Hidano, and S. Kiyomoto, "Sensor-based wearable PUF," in *Proceedings of the 13th International Joint Conference on E-Business and Telecommunications*, ser. ICETE 2016. Setubal, Portugal: SCITEPRESS - Science and Technology Publications, Lda., 2016, pp. 207–214. [Online]. Available: https://doi.org/10.5220/0005946702070214

[14] S. Lee, M.-K. Oh, Y. Kang, and D. Choi, "Design of resistor-capacitor physically unclonable function for resource-constrained IoT devices," *Sensors*, vol. 20, no. 2, 2020. [Online]. Available: https://doi.org/10.3390/s20020404

[15] C. Labrado, H. Thapliyal, S. Prowell, and T. Kuruganti, "Use of thermistor temperature sensors for cyber-physical system security," *Sensors*, vol. 19, no. 18, 2019. [Online]. Available: https://doi.org/10.3390/s19183905

[16] S. Brimah, "Testing LM35 temperature sensors as physical unclonable functions," Master's thesis, University of Passau, 2025.