Sensor Identification via Acoustic Physically Unclonable Function

GIRISH VAIDYA, T. V. PRABHAKAR, and NITHISH GNANI, Indian Institute of Science, India
RYAN SHAH and SHISHIR NAGARAJA, University of Strathclyde, UK

The traceability of components on a supply chain from a production facility to deployment and maintenance depends upon its irrefutable identity. There are two well-known identification methods: an identity code stored in the memory and embedding custom identification hardware. While storing the identity code is susceptible to malicious and unintentional attacks, the approach of embedding a custom identification hardware is infeasible for sensor nodes assembled with Commercially-Off-the-Shelf devices. We propose a novel identifier - `Acoustic PUF` based on the innate properties of the sensor node. `Acoustic PUF` combines the uniqueness component and the position component of the sensor device signature. The uniqueness component is derived by exploiting the manufacturing tolerances, thus making the signature unclonable. The position component is derived through acoustic fingerprinting, thus giving a sticky identity to the sensor device. We evaluate `Acoustic PUF` for Uniqueness, Repeatability, and Position identity with a deployment spanning several weeks. Through our experimental evaluation and further numerical analysis, we prove that `Acoustic PUF` can uniquely identify thousands of devices with 99% accuracy while simultaneously detecting the change in position. We use the physical position of a device within a synthetic sound-field both as an identity measure as well as to validate physical integrity of the device.

CCS Concepts: • **Hardware** → *Hardware reliability*; • **Security and privacy** → *Embedded systems security;*

Additional Key Words and Phrases: Device ID, fingerprinting, physically unclonable function (PUF)

ACM Reference format:
Girish Vaidya, T. V. Prabhakar, Nithish Gnani, Ryan Shah, and Shishir Nagaraja. 2023. Sensor Identification via Acoustic Physically Unclonable Function. *Digit. Threat.: Res. Pract.* 4, 2, Article 20 (August 2023), 25 pages.
https://doi.org/10.1145/3488306

1 INTRODUCTION

The pervasiveness of electronic sensor devices in critical sectors like avionics and automotive is increasing [4, 7, 46]. In the avionics domain, the sensor devices are used in control as well as infotainment systems. Many of the *fully mechanical* systems are incorporating sensor devices. As an example, there is an increased interest in creating smart aircraft latches, in particular, overhead stowage bins mounted with sensor nodes to detect accidental opening and pilferage [5, 41]. Similarly, in the automotive domain, the sensor devices are used in

This work was partially supported by an Aerospace Network Research Consortium (ANRC) grant (BOCO-0018), Department of Science and Technology grant (SP/DSTO-19-0054), and a UKIERI-DST grant (UKIERI2018-19-005). R. Shah is funded by EPSRC (EP/11288S170484-102) and NPL's Data Science program.

Authors' addresses: G. Vaidya, T. V. Prabhakar, and N. Gnani, Department of Electronic Systems Engineering, Indian Institute of Science, Bangalore, Karnataka, India; emails: {vaidyab, tvprabs}@iisc.ac.in, nithishkgnani@gmail.com; R. Shah and S. Nagaraja, Computer and Information Sciences, The University of Strathclyde, Livingstone Tower, 26 Richmond Street, Glasgow, United Kingdom; emails: {ryan.shah, shishir.nagaraja}@strath.ac.uk.

2576-5337/2023/08-ART20 $15.00
https://doi.org/10.1145/3488306

power train, chassis, and body control, as well as infotainment. This increased usage is driving the improvement in efficiency, safety, and overall user experience [3, 46].

As the usage of sensor devices in critical sectors increases, it becomes imperative that these sensor devices are trustworthy and traceable. There is an unmet need for traceability of components and subsystems. Traceability is the mechanism to ensure compliance with operational standards and materials content [17]. Specifically, traceability mandates that (i) the components being used to manufacture the system are traceable to a genuine source. This is addressed by procuring the components through trusted channels, either directly from semiconductor manufacturers or through authorised distributors. Additionally, the semiconductor manufacturer can keep track of parts delivered to end customers through the authorised distributors. This facilitates traceability of counterfeits and compliance to export control. (ii) Well-established production processes are being followed during the assembly of systems and documented at each stage [17]. (iii) In post-production, the sensor device is traceable from the production site till installation and even further during maintenance. Once a system is integrated at a trusted manufacturing facility, the system is tracked throughout its lifetime.

Our work focuses on the traceability of deployed systems (post-production). First, we have to ensure that the sensor device delivered to the customer is the same as the one that was inspected. Second, we must ensure that the device that has delivered a critical message into the workflow is the same that was installed and has not been replaced, either unintentionally or deliberately. Hence it is vital that the devices are identified. This irrefutable identity bootstraps the traceability of the device. Furthermore, it is essential to derive such identification "on the fly" by executing a software **Application Programming Interface (API)**.

One approach to establish the irrefutable identity of the device is through a stored identifier. The identifier is a digital code written into the memory of the device. This identifier could be queried and read back to confirm the identity of the device. Other recent alternatives include dielets [33], DNA fingerprinting [45], and **Physically Unclonable Functions (PUFs)** [22].

An alternate approach that makes use of innate properties of the sensor devices themselves is the use of PUFs. While most of the other solutions attach an "external" identity to the device, PUFs exploit the inherent variations in the manufacturing process to generate unique identification for the devices. Thus, the PUF identity is intrinsic to the device. Semiconductor fabrication involves multiple processes like photolithography, etching, deposition, and so on. Due to the inherent tolerances in these processes, the physical and material properties of the semiconductor components differ slightly from one another. This leads to variation in electrical characteristics of components such as operating frequency, threshold voltage, current consumption, and so on. These variations are exploited to generate signatures. Some prominent examples of PUFs discussed in the literature include Ring oscillator PUF [25, 42], Arbiter PUF [24], and Memory PUFs [20, 44]. While memory PUFs need power cycling [44] to generate the unique signature, other conventional PUFs generate keys through a custom circuit introduced during the silicon manufacturing process. However, limited study has been done on generating PUF signatures for systems assembled from **Commercially-Off-the-Shelf (COTS)** components.

Acoustic techniques have been used to generate fingerprints for device identification [12, 52]. In Reference [52], the android phone generates series of cosine waves from 14 to 21 kHz with a 100-Hz gap between neighbour frequency points. The microphone of the phone itself records the acoustic signal. The spectrum of the recording is analysed to derive the fingerprints of the device. Similarly, in Reference [12], different audio excerpts, including instrumental, human speech, and songs, are given as stimuli. Fifteen different features of the recorded signals, including the signal strength as well as spectral features, are analysed. While these approaches exploit the manufacturing variations in the acoustic components, they do not fingerprint the underlying microcontroller.

We propose a novel `Acoustic PUF` for the identification of devices. `Acoustic PUF` is non-invasive, i.e., it does not need power cycling for generating the identifier. They are attractive, because they are amenable to *in-situ* identification. Furthermore, `Acoustic PUF` works with sensor nodes created from COTS components and thus requires no special hardware. This makes the proposed solution generic enough to be used for bespoke low volume sensor nodes. Since the signature is not integrated into the device during silicon manufacturing, the proposed solution does not solicit any support from the semiconductor manufacturer. Further, in our approach, the microphone does not contribute to the signature. Instead, our approach fingerprints the underlying microcontroller, which is typically the most important component in the system.

In this article, we propose `Acoustic PUF`, consisting of a $Uniqueness_{signature}$ and a $Position_{signature}$, that can differentiate between two device instances of the same type, as well as differentiate when the device is moved from its installed position. In our proposed scheme, the interrogator with an acoustic source gives out periodic pulses of sound. The sensor device, embedded with a microphone, captures these pulses and generates the `Acoustic PUF`. The identity component is extracted by making use of the device process variations, whilst the position component is derived through acoustic fingerprinting. Since the `Acoustic PUF` is derived through the physical characteristics of the manufactured sensor device, it is extremely difficult to replicate the signature, and thus we believe it is a viable solution for identifying these devices while being tracked through the supply chain. We evaluated `Acoustic PUF` across three properties: *repeatability*, *uniqueness*, and *position identity*. Specifically, our work demonstrates the robustness of `Acoustic PUF` for small-scale and mid-scale deployments, and we make the following unique contributions:

- We propose a novel `Acoustic PUF`, capable of identifying the instance of sensor device whilst simultaneously confirming that the device is indeed at its designated position.
- We implement a non-invasive `Acoustic PUF` using commercial off-the-shelf components.
- We evaluate the efficacy of `Acoustic PUF` against the three properties viz. repeatability, uniqueness, and position identity from the results of our deployment of 34 devices.
- We prove the scalability of `Acoustic PUF` for up to 10,000 devices through numerical simulations.

2 ACOUSTIC PUF PROPERTIES AND USE CASES

2.1 Overview

Since `Acoustic PUF` is derived from the innate properties of the sensor node based on manufacturing variations, a similar identifier cannot be systematically created. Further, the probability of two devices having the same identifiers is minimal for a deployment of about 10,000 sensor nodes. This characterises the $Uniqueness$ property of `Acoustic PUF`.

Another important property of `Acoustic PUF` is its ability to provide $Position_{signature}$. Thus `Acoustic PUF` not only tells *who I am* but also provides information about *where I am*. The $Position_{signature}$ is obtained at no additional expense and provides a *sticky* identity to the sensor device. It checks that the sensor device has not moved unexpectedly from its installed position, thus providing it with an additional dimension of security. The novel use of acoustic channel enables the simultaneous generation of $Uniqueness$ and $Position$ signatures. Similar usage of RF channel while provides the $Uniqueness$ information, it fails to provide any information regarding $Position$. We believe this is the first work providing an integrated approach to generate $Uniqueness$ and $Position$ signature using PUF.

We envisage that the generated $Position_{signature}$ could be used to (i) further strengthen the identity and (ii) enable novel applications that combine $Uniqueness$ and $Position$ information together to drive anomaly detection. In Section 2.2, we present one such use-case for detecting the unauthorised opening of armed latches, such as stowage bin latch in an aircraft.

Many applications demand the deployment of multiple sensors of similar types at different positions. Any replacement of a calibrated sensor with an uncalibrated one or accidental swapping in the position of sensors may cause incorrect decisions leading to potential safety hazards. As an example, in an aircraft, there are multiple fuel tanks with their respective gauges to indicate the fuel level. It is critical to confirm the calibration status of the sensor and its position before undertaking any action based on the alert issued by the sensor. As another example, physical movement of sensitive oscilloscopes, used in the production and testing of semiconductor ICs, is enough to render them miscalibrated. By deploying `Acoustic PUF`, any unauthorised movement will

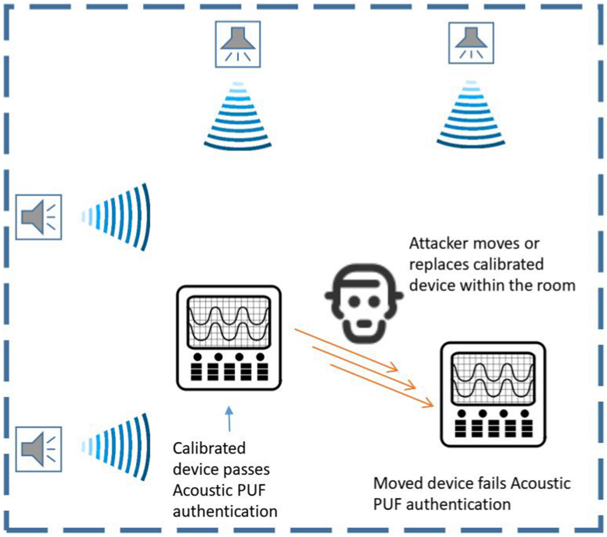

Attacker moves or replaces calibrated device within the room
Calibrated device passes Acoustic PUF authentication
Moved device fails Acoustic PUF authentication

Fig. 1. Monitoring the calibration-integrity of sensor-network deployment using Acoustic PUF.

immediately be detected and the oscilloscope will be disallowed from further participation on the production line, avoiding significant reputational and financial losses by preventing a product recall. To return to service, the oscilloscope will have to be recalibrated and a new `Acoustic PUF` identity generated to confirm fitness-for-purpose before it is returned to the production workflow. We will systematically discuss this example as a use-case in Section 2.3.

2.2 Usecase: Stowage Bin Latch

We construct a *smart aircraft latch* integrating the $Uniqueness$ and $Position$ signatures. Such a device is a subject of ongoing studies [5, 41]. Our work takes the existing body of work further by proposing a solution wherein the same sensor device could also be used to secure the latches while the aircraft is parked.

We consider a scenario when the aircraft is parked in the bay for maintenance. Typically, the periodic C-check for an aircraft is performed after a specified number of flying hours. This check involves individual systems and components limited to the Electronic and Equipment bay. However, reports indicate that the overhead stowage latches in the cabin area are found to be tampered. Our proposed approach has the ability to detect the opening of stowage bins by a suitable mechanical mounting arrangement of sensor nodes that get displaced from their armed positions in the event of a latch tamper.

We propose that the existing speakers are used as acoustic sources. While the aircraft is getting parked, the sensor devices are armed, and the $Uniqueness$ and the $Position$ signatures for all the sensor devices are collected. The highlight of the proposed solution is that the sensor devices need not stay armed during the entire duration when the aircraft is parked, i.e., they could be powered down. Before the next flight of the aircraft, the sensor devices are reactivated during the security check. Any change in $Position_{signature}$ not only detects the opening of the stowage bin but also provides information about the specific stowage bin that was tampered with. Our evaluation shows that a displacement of as small as 5 cm could generate a detectable difference in $Position_{signature}$. Thus the tamper detection and position of the stowage bin could be obtained by the interrogator in real time and does away with manual checks. Further, the $Uniqueness_{signature}$ avoids any attempted pilferage. If the *original* sensor device is replaced by a *fake* device with an intention to bypass the check, then such a replacement could be detected through the $Uniqueness_{signature}$. Thus by combining the $Uniqueness_{signature}$ and the $Position_{signature}$ of the `Acoustic PUF`, the overhead stowage bins are secured.

2.3 Use Case: Monitoring the Calibration-Integrity of an IoT/Sensor-Network Deployment

As IoT deployments become pervasive, the reliability of their operation becomes an important safety requirement. Calibration is an important and necessary step that bootstraps system reliability. Understanding when a subset or whole of an IoT deployment enters the miscalibrated state is therefore important for the system operator. As deployment scales, it can get challenging for the operator to ensure calibration of a deployment. Mapping device measurements back to the device's calibration status requires unambiguous identification of the device, which motivates the use of a PUF.

Ensuring calibration within a deployment is challenging. First, the scale of deployments may exceed the ability of the manual calibration regimes where each device is calibrated against a more accurate device. Second, between periodic calibration cycles, the devices may enter a miscalibrated status due to intentional or unintentional failures. `Acoustic PUF` effectively solves the challenge of monitoring the calibration status of a deployment by actively monitoring device identities as a function of each device's physical integrity within a deployment.

Calibration is the process of comparing a measurement or instrumentation device against a more accurate device to understand its deviation profile. By applying appropriate offsets to measurements generated by the device, the deviations from "true readings" are minimised, thus increasing reliability. Periodic calibration is usually required to refresh the deviation profile and generate fresh calibration offsets to minimise measurement uncertainty.

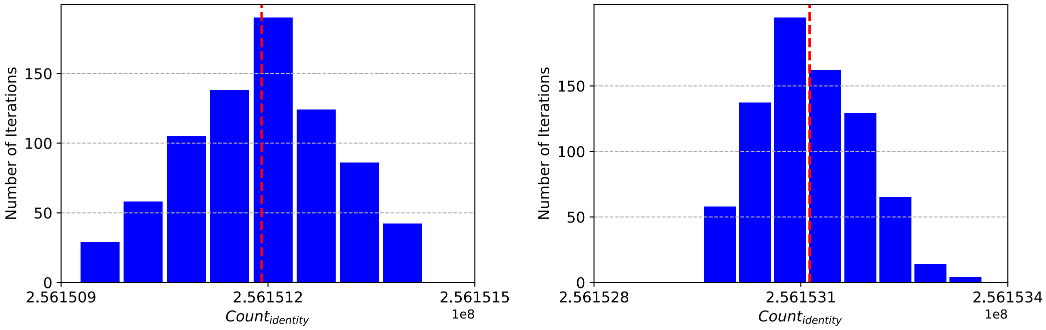
However, periodic calibration guards against miscalibration only when the physical integrity of the device is not compromised [6, 35, 37]. There are primarily two sub-classes of failures that can compromise physical integrity: unintentional failures (stochastic events) and intentional failures (attacks). First, unintentional failures such as physical shocks or careless swapping out of devices by operators may result in uncalibrated devices entering the workflow. In the case of sensitive devices, the merely shifting devices may render them uncalibrated [6, 43] as a small force is enough to disturb physical integrity. Second, intentional miscalibration is caused by an attacker such as a malicious or disgruntled employee. Attackers seek plausible deniability to protect themselves from attribution, motivating a preference for stealthy attacks. We note that inducing miscalibration can be done stealthily by simply moving the target device from its calibrated location or subjecting it to physical shocks (which involves temporary device movement as well).

In both unintentional failures and (stealthy) intentional failures, we note that the target device experiences location movement. We posit that monitoring location movement can offer useful information about physical integrity and hence calibration status. While this is easy enough for purpose-built devices, how can we carry out reliable location-inference for devices within existing deployments? `Acoustic PUF` positively identifies a device based both on its physical and location characteristics, making it a suitable mechanism for detecting when a subset of a deployment is entering miscalibration status. Figure 1 shows one such scenario wherein `Acoustic PUF` is used to detect the deployment entering miscalibration when an attacker moves or replaces a calibrated device. During installation, `Acoustic PUF` is generated using the acoustic infrastructure consisting of the speakers in the room and the microphones on the calibrated instrument. Periodically, the signature is regenerated to confirm the calibration integrity. The location change is detected by the altered $Position_{signature}$, whereas $Uniqueness_{signature}$ detects any replacement. Moreover, `Acoustic PUF` is a fully passive technique and can work on-the-fly without operator initiative beyond the initial mechanism configuration process.

2.4 `Acoustic PUF` Properties

We evaluate `Acoustic PUF` across the following key properties:

(1) **Repeatability:** There is little variation in the signature of the device if queried repeatedly due to the inherent device and measurement noise. This intra-device signature variation should lie within an acceptable threshold.



(a) Device 1: $Count_{identity}$

(b) Device 2: $Count_{identity}$

Fig. 2. Histogram of $Count_{identity}$ for two devices.

(2) **Uniqueness:** Each device should generate a signature that is different from the other device. The inter-device signature variation should be large enough so that thousands of devices could be uniquely identified. The uniqueness of the device is captured in the $Uniqueness_{signature}$ part of `Acoustic PUF`.

(3) **Position identity:** The sensor device should convey information about its position as part of the signature. If the sensor device is displaced, then the signature should change. The position of the device is captured in the $Position_{signature}$ of the `Acoustic PUF`.

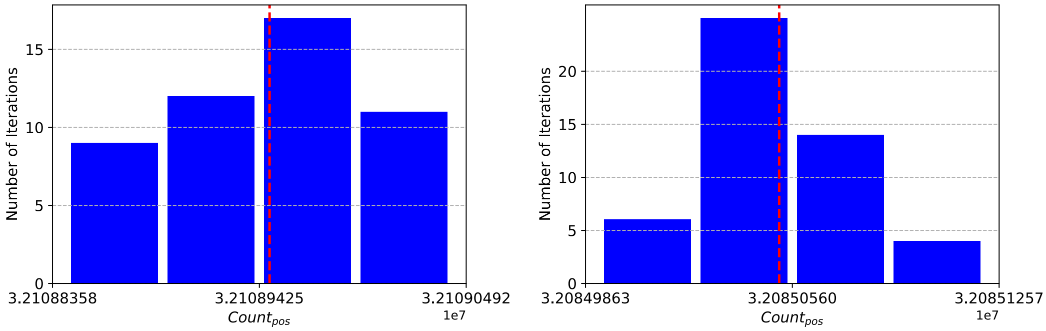
`Acoustic PUF` combines $Uniqueness_{signature}$ and $Position_{signature}$ to create a strong device identity.

2.4.1 $Uniqueness_{signature}$ for `Acoustic PUF`. Clock is ubiquitous in all digital systems, and all activities are synchronised over the clock ticks. Most of the modern microcontrollers have more than one independent clock source [11, 32]. Further, clock dividers and **phase-locked loops (PLLs)** are used for generating derived clocks.

Due to variations in the manufacturing process of these clock sources and dividers, the clock frequency varies from one device instance to another. The variation is typically in the range of a few hundred ppm for crystal-based clocks and extends up to ±8% for internal on-chip oscillator clocks [32]. Hence if the count of clock ticks viz., $Count_{identity}$ is measured across two different clock devices for the same time duration, then this number would be slightly different. We generate the $Uniqueness_{signature}$ exploiting this difference in clocks. Specifically, we generate single tones spaced at 16 seconds and measure this time duration using the timer circuit in the sensor device. The single tones are broadcasted by the interrogator through an acoustic source and captured by the sensor devices through a microphone. Two independent clocks, viz. crystal oscillator and internal oscillator, are used by the timer circuit as a source for the measurement. Further, to improve the uniqueness, aggregation over a sliding window of eight such successive counts is performed to create the $Uniqueness_{signature}$. As an example, $Count_{identity}$ with sequence numbers 1–8 are aggregated to generate the first $Uniqueness_{signature}$ and $Count_{identity}$ with sequence numbers 2–9 are aggregated to generate the next $Uniqueness_{signature}$. We also note the temperature to account for variation in the count with respect to temperature. Hence $Uniqueness_{signature}$ is a tuple defined as

$$Uniqueness_{signature} = \left(\sum_{1}^{8} Count_{identity-cry}, \sum_{1}^{8} Count_{identity-int}, Temperature\right), \quad (1)$$

where $Count_{identity-cry}$ and $Count_{identity-int}$ represent the $Count_{identity}$ for crystal oscillator and internal oscillator, respectively. Figure 2 shows the histogram of $Count_{identity-cry}$ measured over a duration of 16 seconds for two different devices of the same hardware for 700 readings. The two devices have identical embedded software code. The x-axis represents the $Count_{identity}$ and the y-axis represents the number of iterations. The red line indicates the statistical mean. Device 1 has an average of 256,151,190, and Device 2 has an average of 256,153,112



(a) Position 1: $Count_{pos}$

(b) Position 2: $Count_{pos}$

Fig. 3. Histogram of $Count_{pos}$ for two positions.

with a standard deviation within 100. The small standard deviation proves the repeatability property. Thus, it is possible to distinctly identify these two devices based on the $Uniqueness_{signature}$ generated by accumulating the $Count_{identity}$.

2.4.2 $Position_{signature}$ for `Acoustic PUF`*.* Consider a setup where two fixed acoustic sources are kept at a distance from each other at predetermined points S1 and S2. The source at point S1 generates a tone followed by the source at point S2. A sensor device at position D receives the two tones and calculates the time difference between their arrivals. This **time difference of arrival (TDOA)** would differ based on the relative position of D with reference to S1 and S2. We exploit this difference in TDOA to create fingerprints for the positions. Specifically, we generate three fingerprints viz., $Count_{pos}$ using four acoustic sources. Two such sets of three $Count_{pos}$ each are obtained from two independent oscillators together forming $Position_{signature}$. We also note the temperature to account for variation in the count with respect to temperature. Section 4.2 provides further details regarding the methodology for signature generation. Hence $Position_{signature}$ is a tuple defined as

$$\begin{aligned} Position_{signature} = \Big(&Count_{pos-cry-P3P4}, Count_{pos-cry-P3P5}, Count_{pos-cry-P3P6}, \\ &Count_{pos-int-P3P4}, Count_{pos-int-P3P5}, Count_{pos-int-P3P6}, Temperature\Big), \end{aligned} \quad (2)$$

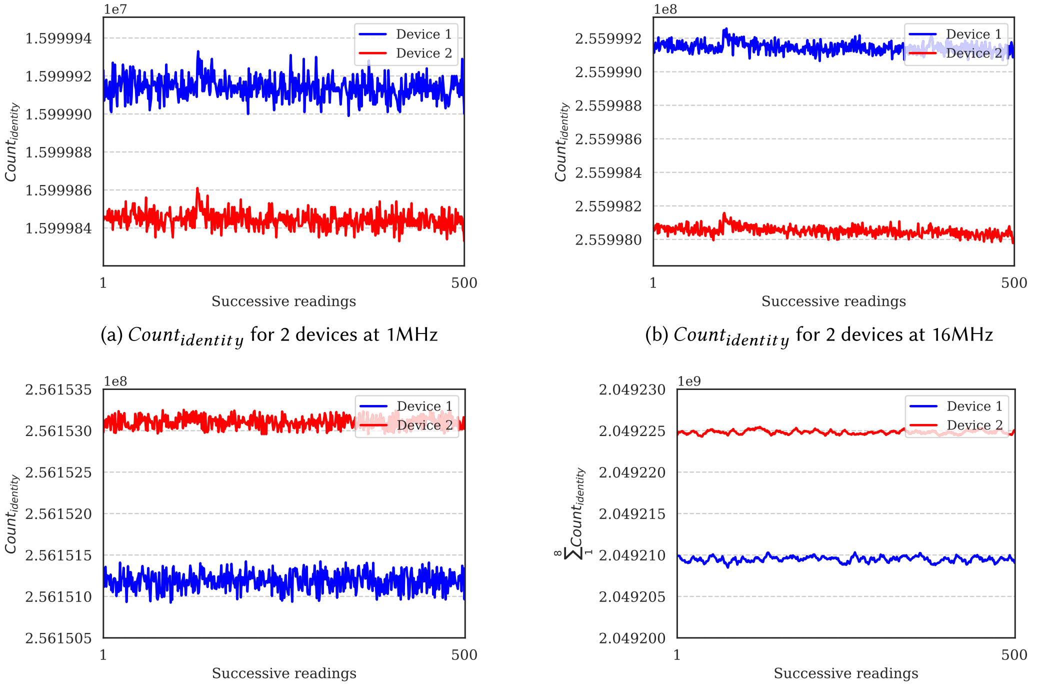
where $Count_{pos-cry-PiPj}$ and $Count_{pos-int-PiPj}$ represent the $Count_{pos}$ between pulses i and j for crystal oscillator and internal oscillator, respectively. We observe that the $Count_{pos}$ varies from one position to another, generating distinct $Position_{signature}$ for each position.

Figure 3 shows the histogram of $Count_{pos}$ for the same sensor device installed at two different positions 50 cm apart. The x-axis represents the $Count_{pos}$, and the y-axis represents the number of iterations. The red line indicates the statistical mean. We observe that the average count at position 1 is 32,108,946, and the average count at position 2 is 32,085,052. The standard deviation of the count at both positions is within 50 counts. The small standard deviation proves the repeatability property. Thus it is possible to identify the position uniquely through $Position_{signature}$ generated by $Count_{pos}$.

2.5 Parameters Impacting `Acoustic PUF`

There are two parameters to be configured while generating `Acoustic PUF`, viz., the timer frequency and the accumulation count.

2.5.1 Timer Frequency. As the clock frequency increases, the timer accumulates more counts within the same time duration. In many microcontrollers, this clock frequency is programmable. Figures 4(a) and (b) plot



(a) $Count_{identity}$ for 2 devices at 1MHz

(b) $Count_{identity}$ for 2 devices at 16MHz

(c) $Count_{identity}$ for 2 devices with no accumulation

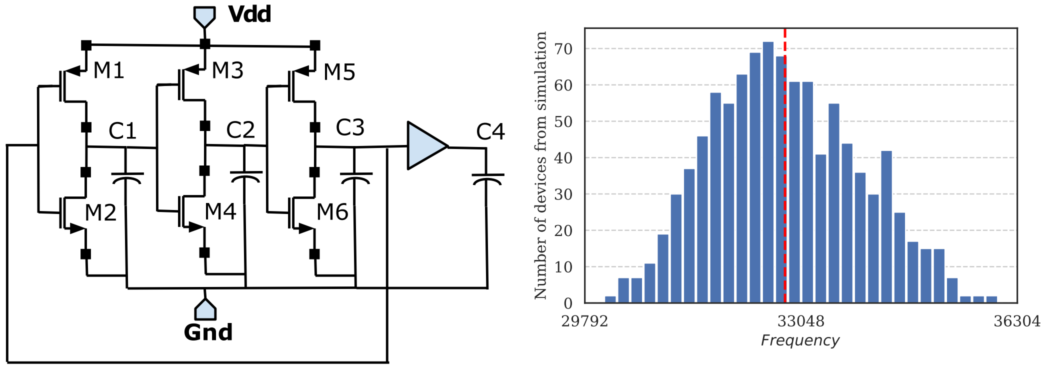
(d) $Count_{identity}$ for 2 devices with accumulation=8

Fig. 4. Impact of timer frequency and accumulation on $Count_{identity}$.

$Count_{identity}$ over 16-second duration for clock frequencies of 1 MHz and 16 MHz, respectively, using a crystal oscillator as the source. The standard deviation is within five counts for 1 MHz and within 40 counts for 16 MHz. However, the statistical mean count is of the order of 16,000,000 for 1 MHz and 256,000,000 for 16 MHz. Thus, while the standard deviation has scaled eight times, the statistical mean for both devices has scaled 16 times, providing an improved separation. Hence we recommend using a higher clock frequency for generating the signatures.

2.5.2 Accumulation Count. As discussed in Section 2.4.1, we accumulate eight $Count_{identity}$ counts for generating the $Uniqueness_{signature}$. Figures 4(c) and (d) demonstrate the impact of accumulation count. In Figure 4(c), no accumulation is done. In Figure 4(d), eight $Count_{identity}$ counts are accumulated to create the $Uniqueness_{signature}$. The statistical mean for the $Count_{identity}$ in Figure 4(c) is of the order of 256,100,000, and in Figure 4(d) the statistical mean of the accumulated $Count_{identity}$ is of the order of 2,049,000,000. The corresponding standard deviations are within 90 and 270, respectively. Thus, the statistical mean has scaled eight times, whereas the standard deviation has scaled three times. This demonstrates that the separation improves with the increase in accumulation. When **N** number of accumulations are performed, while the mean scales linearly with **N**, the standard deviation scales $\sqrt{N}$. Thus, the coefficient of variation decreases to improve the repeatability [47].

In summary, improved separation could be achieved by increasing the timer frequency and accumulation count. Increasing the timer frequency improves the signature without increasing the time required for signature generation. However, increasing the accumulation count increases the latency for signature generation. On the contrary, while the timer frequency is limited by the hardware, the accumulation count may be increased



(a) 3 stage Ring oscillator

(b) Histogram of frequency

Fig. 5. Monte Carlo simulations for ring oscillator.

arbitrarily within acceptable signature generation time limits. We further discuss the impact of accumulation count while discussing scalability in Section 6.

While we have discussed the impact of timer frequency and accumulation on $Uniqueness_{signature}$, there is a similar impact on $Position_{signature}$. For our experimental evaluation, we have considered a timer frequency of 16 MHz and an accumulation count of 8.

3 THE THEORY BEHIND ACOUSTIC PUF

In this section, we demonstrate the working principle of Acoustic PUF through sample simulations.

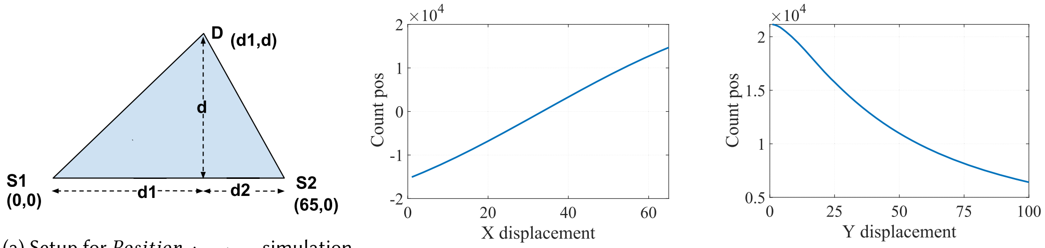
3.1 Circuit Simulations for $Uniqueness_{signature}$ Generation

The variation in clock frequency across devices is exploited for the $Uniqueness_{signature}$ generation. We present circuit simulations to understand how the device variations impact the frequency of a clock oscillator. We use a three-stage ring oscillator architecture for the clock, as shown in Figure 5(a). Each stage consists of an inverter and a capacitive load. This is one of the standard architectures for oscillator implementation [51]. The clock oscillator generates a 32.768-kHz clock during a typical simulation. The circuit design is implemented and simulated using an industry-standard LTspice simulator [13].

The values of the capacitors and the physical dimensions of the transistors (W, L) are modeled to have a tolerance of 10%. We performed Monte Carlo simulations for 1000 iterations; each iteration represents a separate device with capacitance value and transistor dimensions picked up randomly, drawn through uniform distribution within the specified tolerance range. More details about the Monte Carlo simulation methodology are available in Reference [14]. Figure 5(b) plots the histogram of clock frequency distribution across 1,000 devices from the circuit simulation of the clock oscillator. The bin width considered for the histogram is 100 Hz. From Figure 5(b), we observe that the frequency varies from 30 to 36 kHz with a 3σ deviation of 10.2% and a statistical mean of 32.8 kHz. If this ring oscillator is considered as a clock source to timer across different devices, then the number of counts measured in a certain duration will have identical distribution. The devices falling within the same bin could be differentiated further by accumulating the clock counts and considering multiple clock sources, as discussed in Section 2.5. The Monte Carlo simulations of a ring oscillator with 0.18-μm devices from UMC report a similar frequency variation [47].

3.2 Numerical Simulation for $Position_{signature}$ Generation

We present numerical simulations in MATLAB to demonstrate the change in $Position_{signature}$ when the sensor device is displaced. The setup considered is as shown in Figure 6(a). Two acoustic sources, S1 at (0,0) and S2



(a) Setup for $Position_{signature}$ simulation

(b) X displacement impact

(c) Y displacement impact

Fig. 6. Principle of $Position_{signature}$ generation.

at (65,0), are placed 65 cm apart. The sensor device D is at a perpendicular distance d from the line connecting S1 and S2. The distance S1-D is $Dist_{S1-D} = \sqrt{d1^2 + d^2}$. Similarly, the distance S2-D is $Dist_{S2-D} = \sqrt{d2^2 + d^2}$. In this case, the TDOA is $T_{TDOA} = (Dist_{S1-D} - Dist_{S2-D})/v$ where v is the velocity of sound. The corresponding difference in $Count_{pos}$ is $T_{TDOA} * f$ where f is the frequency of the clock oscillator on the sensor device. f is assumed as 16 MHz for this simulation and v is 340 m/s.

Figure 6(b) plots the $Count_{pos}$ values when Device D is moved in the X direction from (0,d) to (65,d) parallel to the line connecting S1 and S2. d is assumed as 50 cm for this simulation. Similarly, Figure 6(c) plots the $Count_{pos}$ values when the Device D is moved in the Y direction from (55,0) to (55,100). Plots 6(b) and 6(c) show that when D is displaced in the XY plane, $Position_{signature}$ are generated due to a difference in TDOA values.

As explained in Section 2.4.2, we generate $Position_{signature}$ using four different acoustic sources. This ensures that the position is uniquely identified in a two-dimensional 2D plane. This approach could be further extended to identify the position uniquely in a 3D plane by the appropriate placement of more acoustic sources.

RF signal vs. Acoustic signal for $Position_{signature}$: The velocity of a sound wave in air is 340 m/s. The velocity of an RF wave in air is 300×10^6 m/s, thus six orders higher than a sound wave. Thus the $Count_{pos}$ with an RF wave would be six orders lower than the corresponding $Count_{pos}$ generated through a sound wave. Hence generating distinct $Position_{signature}$ using an RF wave is practically infeasible. In Figure 6(b), the sensor device D will have the same $Count_{pos}$ of 0 across all positions on the line connecting S1 and S2 if an RF signal is used instead of an acoustic signal.

4 SYSTEM OVERVIEW

In this section, we discuss the setup infrastructure used to carry out the experiments. We provide details about the hardware devices and the software APIs used.

4.1 Sensor Devices

The embedded sensor devices typically consist of a (i) Sensor, (ii) Analog signal conditioning circuit, (iii) Microcontroller core, (iv) Power regulation circuit, and (v) Communication module. Most of these sensor devices are built from COTS components, chosen and assembled together on a PCB to meet the required functionality and performance specifications.

The sensor device used in our experiments is as shown in Figure 7. The microphone used is ICS-40618 from Invensense [21]. The microphone is connected to the microcontroller board through a custom signal conditioning board. The signal conditioning board has an amplifier and a filter circuit. The output of the signal conditioning board connects to one of the analog comparator inputs on the microcontroller board. The microcontroller board detects a pulse when the input acoustic signal crosses a preset threshold value.

Specifically, for our experiments, we have considered 34 sensor devices from two different microcontroller device families

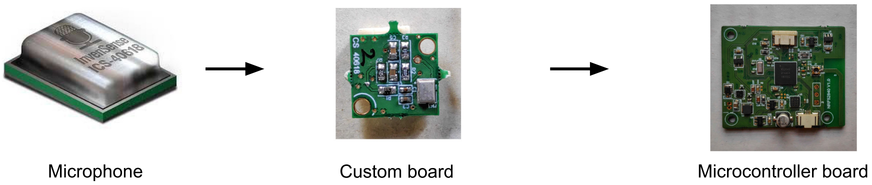
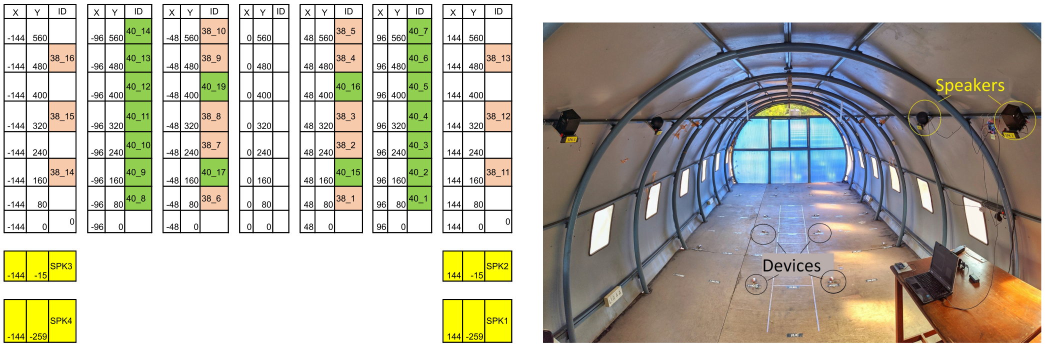


Fig. 7. Components of sensor device.



X	Y	ID	X	Y	ID	X	Y	ID	X	Y	ID	X	Y	ID	X	Y	ID	X	Y	ID
-144	560		-96	560	40_14	-48	560	38_10	0	560		48	560	38_5	96	560	40_7	144	560	
-144	480	38_16	-96	480	40_13	-48	480	38_9	0	480		48	480	38_4	96	480	40_6	144	480	38_13
-144	400		-96	400	40_12	-48	400	40_19	0	400		48	400	40_16	96	400	40_5	144	400	
-144	320	38_15	-96	320	40_11	-48	320	38_8	0	320		48	320	38_3	96	320	40_4	144	320	38_12
-144	240		-96	240	40_10	-48	240	38_7	0	240		48	240	38_2	96	240	40_3	144	240	
-144	160	38_14	-96	160	40_9	-48	160	40_17	0	160		48	160	40_15	96	160	40_2	144	160	38_11
-144	80		-96	80	40_8	-48	80	38_6	0	80		48	80	38_1	96	80	40_1	144	80	
-144	0	0	-96	0		-48	0		0	0		48	0		96	0		144	0	0
-144	-15	SPK3																144	-15	SPK2
-144	-259	SPK4																144	-259	SPK1

(a) Installation positions

(b) Acoustic PUF testbed

Fig. 8. Deployment setup of sensor devices.

(1) Device type D1: 18 numbers of custom boards with nRF52840 microcontroller from Nordic semiconductors. The nRF52840 microcontroller has an internal high and low-frequency oscillator, PLL, and comparator [32].
(2) Device type D2: 16 numbers of custom boards with nRF52832 microcontroller from Nordic semiconductors [31].

4.2 Experimental Setup

Figure 8 shows the installation of sensor devices and speakers laid out in a grid fashion over a 2.88 m × 5.6 m area. The grid arrangement of sensor devices evaluates the generic nature of the proposed approach to generate $Position_{signature}$. The X and Y numbers in Figure 8(a) indicate the (X, Y) coordinates of the speakers and the sensor devices measured in centimetres; the origin indicated by (0, 0). All the sensor devices are in the same XY plane with Z coordinate = 0. Figure 8(b) shows that four speakers viz. SPK1, SPK2, SPK3 and SPK4, used as acoustic sources are installed at positions $(-144, -15)$, $(-144, -259)$, $(144, -15)$ and $(144, 259)$; all with Z coordinate = 200. The experimental setup does not assume a line of sight between the acoustic sources and the sensor nodes, thus accounting for the multipath environment. This mimics the deployment conditions in the field.

The speakers are driven through a single controller, viz. nRF52832-DK development board for Nordic 52832 microcontroller [39]. The usage of a single microcontroller eliminates any need for synchronisation across different acoustic sources. The embedded board driving the speakers is programmed to generate a pulse train with a 1-kHz tone for specified durations and at specific intervals, as shown in the timing diagram Figure 9. The crystal-based clock source is used for generating the timings, thus reducing the tolerance and jitter during pulse generation.

Figure 9 shows the timing diagram of the pulse pattern used for the generation of signatures. Speaker SPK1 generates start pulse P1 of 1 seconds followed by two pulses P2 and P3 of 0.1 seconds each, separated by 16 seconds. Speaker SPK2 generates a pulse P4 of 0.1 seconds, 2 seconds after P3. Similarly, speakers SPK3 and

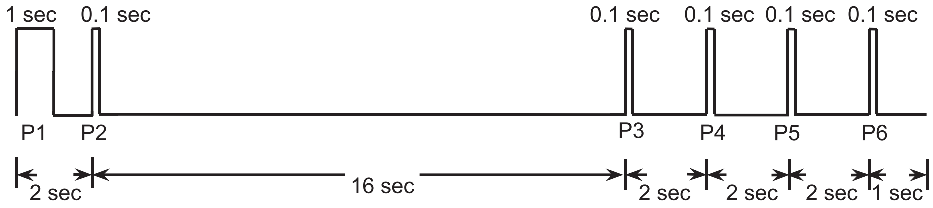


Fig. 9. Timing of audio pulses.

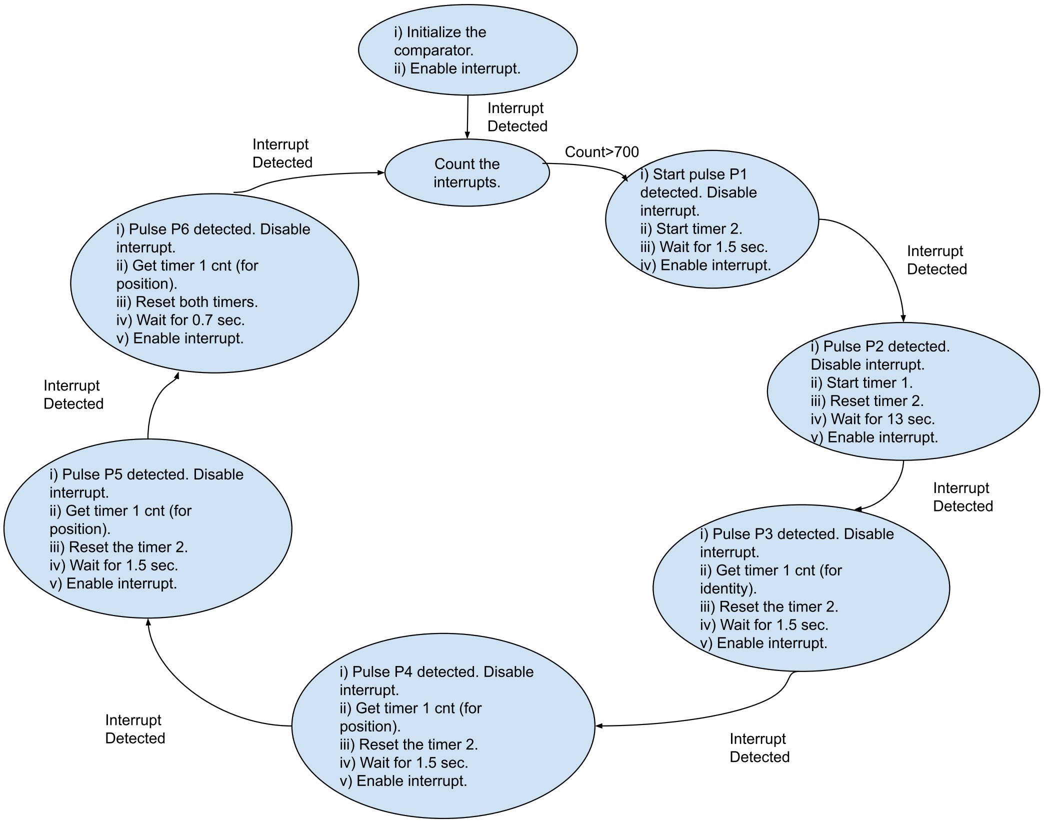


Fig. 10. State diagram of API for extraction of signatures.

SPK4 generate pulses P5 and P6, separated by a 2-second interval. During the pulse duration, the corresponding speaker sends out a single tone of 1 kHz. The duration of 16 seconds has been chosen heuristically. A longer duration causes better distinction amongst the devices at the expense of increased time for signature generation.

We have developed an API to extract the sensor device signatures. The functionality of the API is captured in the state diagram in Figure 10. To avoid false triggering due to external noise sources, a threshold determined empirically is used. The presence of an input tone is detected by the comparator whenever the 1-kHz input signal crosses the preset threshold. Every crossing of input cycle causes an interrupt. The start of signalling is indicated by a start pulse P1. The detection of 700 input cycles corresponding to 0.7 seconds is recognised as a valid start pulse. Pulse P2 triggers the signature generations by starting the internal timer T1. The T1 count is noted when pulses P3, P4, P5, and P6 are detected. Another timer T2 is used for disabling the interrupt for specific intervals between the pulses. The interrupts are disabled for 1.5 seconds during 2-second intervals (e.g., between P1 and P2), and 13 seconds during 16-second intervals (between P2 and P3) to prevent interrupts from being caused by spurious signals. The count difference between P2 and P3 provides the $Count_{identity}$ and the count differences among P3-P4, P3-P5, and P3-P6 provide the three $Count_{pos}$ viz. $Count_{pos-P3P4}$, $Count_{pos-P3P5}$ and $Count_{pos-P3P6}$ for $Position_{signature}$. The $Count_{identity}$ and $Count_{pos}$ are measured for both internal oscillator and crystal oscillator during alternate cycles, adding to the robustness of signatures.

4.3 Usage Model

During the pre-deployment phase, the positions of the sensor devices and the acoustic sources are carefully planned based upon the application. The sensor devices are connected to a master device over a communication channel, either wired or wireless. The trained **machine learning (ML)** model is deployed in the master device.

During the deployment phase, the sensor devices count the $Count_{identity}$ and $Count_{pos}$ and communicate them to the master device. The master device runs the ML algorithm and performs the identification and positioning of the sensor devices. Any further action, like creating alerts, is taken by the master device.

The implementation of ML algorithms for resource-constrained embedded nodes is now supported [23]. Thus alternatively, the ML algorithm could also be executed locally in the sensor nodes, and the final identification and position information could be communicated to the master device.

5 EXPERIMENTAL EVALUATION AND RESULTS

In this section, we evaluate the Uniqueness, Position identity, Repeatability and Accuracy of `Acoustic PUF`.

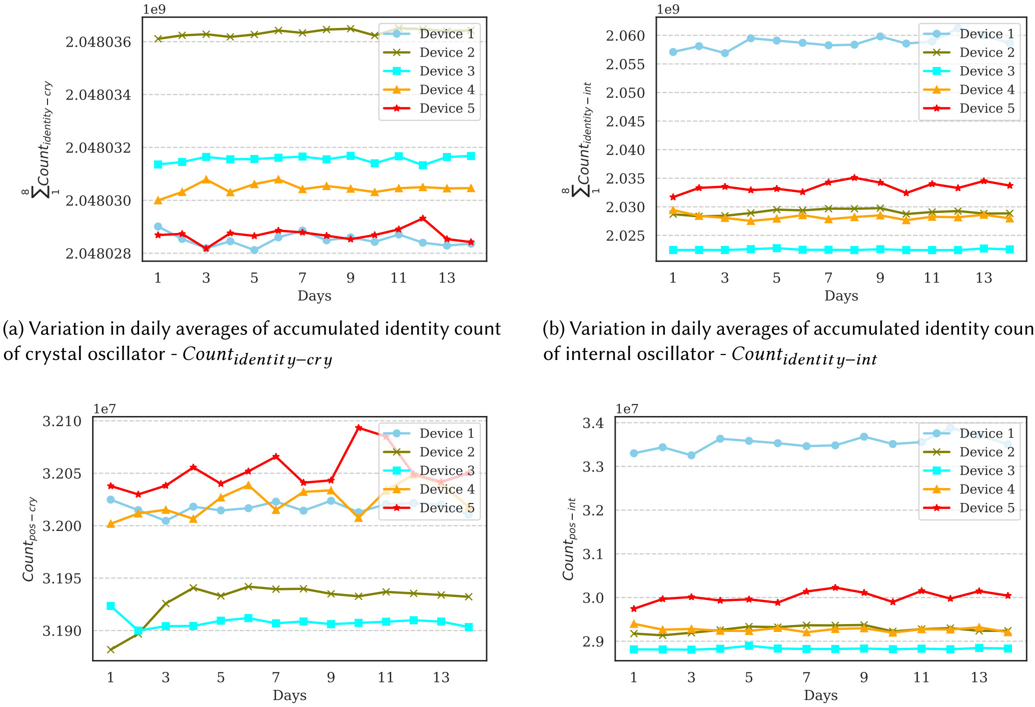
Data collection: Figure 8 captures the picture of the setup during the deployment. We deployed 34 sensor devices in the indoor environment distributed over an area of 2.88 m × 5.6 m, exposed to the ambient temperature. The ambient temperature varied between 15°C and 45°C during the deployment duration. To manage the existing hardware resources, the devices were split into batches and data was collected for each batch for two weeks over a period of three months. Over this deployment duration, we have collected more than 400K data points for each of the counts. Specifically, 400K values each of $Count_{identity-cry}$, $Count_{pos-cry-P3P4}$, $Count_{pos-cry-P3P5}$, $Count_{pos-cry-P3P6}$, $Count_{identity-int}$, $Count_{pos-int-P3P4}$, $Count_{pos-int-P3P5}$ and $Count_{pos-int-P3P6}$ were collected along with corresponding temperatures. The $Uniqueness_{signature}$ and $Position_{signature}$ were computed from these values by aggregation of eight successive counts over a sliding window.

5.1 Uniqueness and Repeatability of `Acoustic PUF`

We present the results to show the uniqueness of `Acoustic PUF`. Figures 11(a) and (b) plot the daily averages for accumulated $Count_{identity-cry}$ and accumulated $Count_{identity-int}$ respectively over the deployment duration. The x-axis represents the time in days, and the y-axis represents the daily average of accumulated $Count_{identity}$. Each line represents a separate device. We observe that: (i) Due to the tolerance in the manufacturing process, the accumulated $Count_{identity}$ varies from one device to another. This confirms the uniqueness property of `Acoustic PUF`. (ii) For each device, the daily average varies minimally. This confirms the repeatability property of `Acoustic PUF`. (iii) There is some overlap for certain devices. As an example, in Figure 11(a), we observe that Device 1 and Device 5 $Count_{identity-cry}$ curves overlap. However, the same devices show distinct $Count_{identity-int}$ curves in Figure 11(b). Thus, their $Uniqueness_{signature}$ are distinct.

5.2 Position Identity and Repeatability of `Acoustic PUF`

We present the results to show the position identity of `Acoustic PUF`. Figures 11(c) and 11(d) plot the daily averages of $Count_{pos-cry-P3P4}$ and $Count_{pos-int-P3P4}$ across five positions over the deployment duration. The x-axis represents the time in days and the y-axis represents the daily average of $Count_{pos}$ over days. Each line represents a different position. We observe that (i) the $Count_{pos}$ varies from one position to another. This confirms the position identity property of `Acoustic PUF`. (ii) For each individual position in the installation, the daily average



(a) Variation in daily averages of accumulated identity count of crystal oscillator - $Count_{identity-cry}$

(b) Variation in daily averages of accumulated identity count of internal oscillator - $Count_{identity-int}$

(c) Variation in daily averages of position count of crystal oscillator - $Count_{pos-cry}$

(d) Variation in daily averages of position count of internal oscillator - $Count_{pos-int}$

Fig. 11. Repeatability and uniqueness for identity and position signatures.

varies minimally over days. This confirms the repeatability property of `Acoustic PUF`. (iii) Figure 11(c) shows little noise in the $Count_{pos-cry-P3P4}$, i.e., variation in values over days. However, we discuss in Section 5.3 that the position is identified accurately despite the noise, since six $Count_{pos}$ are considered together for generating the $Position_{signature}$.

5.3 Accuracy of $Uniqueness_{signature}$ and $Position_{signature}$

In this section, we evaluate the accuracy of `Acoustic PUF` to identify a sensor device and its position.

We have collected more than 400K data points across the sensor devices. We use a ML classification model to confirm the efficacy of $Uniqueness_{signature}$ and $Position_{signature}$. Specifically, we use a kNN model with $k = 30$ and perform 10-fold cross-validation to evaluate the accuracy. We perform analysis under three different cases by redefining $Uniqueness_{signature}$ and $Position_{signature}$ and further evaluate the impact of a subset of features for each of the cases. The accuracy numbers for each of the cases are summarised in Tables 1 and 2.

5.3.1 Case 1: No Accumulation. In this case, the $Uniqueness_{signature}$ and $Position_{signature}$ is a tuple of $Count_{identity}$ and $Count_{pos}$ without accumulation. The signatures at one single temperature are considered as features, i.e.,

$$Uniqueness_{signature} = \left(Count_{identity-cry}, Count_{identity-int}, Temperature\right), \tag{3}$$

$$\begin{aligned} Position_{signature} = \big(&Count_{pos-cry-P3P4}, Count_{pos-cry-P3P5}, Count_{pos-cry-P3P6}, \\ &Count_{pos-int-P3P4}, Count_{pos-int-P3P5}, Count_{pos-int-P3P6}, Temperature\big). \end{aligned} \tag{4}$$

Table 1. Accuracy Percentage Output from ML: $Uniqueness_{signature}$ for Different Cases

Features	**Case-1**	**Case-2**	**Case-3**
All features: Internal osc, crystal osc and temperature	76.8	89.7	99.4
No crystal osc, only internal osc and temperature	50.6	58.54	99
No internal osc, only crystal osc and temperature	21.7	35.7	89.3
No temperature, only internal osc and crystal osc	57.1	71.7	95.4

Table 2. Accuracy Percentage Output from ML: $Position_{signature}$ for Different Cases

Features	**Case-1**	**Case-2**	**Case-3**
All features: internal osc, crystal osc and temperature	98.5	99.7	99.9
No crystal osc, only internal osc and temperature	85.2	91	99.4
No internal osc, only crystal osc and temperature	96.9	97.2	99.4
No temperature, only internal osc and crystal osc	98.5	99.5	99.8

As observed in Tables 1 and 2, the $Uniqueness_{signature}$ and $Position_{signature}$ yields an accuracy of 76.8% and 98.5%, respectively, when all the features are considered. The $Uniqueness_{signature}$ accuracy reduces significantly when only two features are considered. The $Position_{signature}$ in comparison stays greater than 85% even when one of the features is excluded.

5.3.2 Case 2: Accumulation of 8. In this case, the $Uniqueness_{signature}$ and $Position_{signature}$ are tuples generated by accumulating eight corresponding *Counts*. The signatures at one single temperature are considered as features, i.e.,

$$Uniqueness_{signature} = \left(\sum_{1}^{8} Count_{identity-cry}, \sum_{1}^{8} Count_{identity-int}, Temperature \right), \tag{5}$$

$$\begin{aligned} Position_{signature} = \Bigg(& \sum_{1}^{8} Count_{pos-cry-P3P4}, \sum_{1}^{8} Count_{pos-cry-P3P5}, \sum_{1}^{8} Count_{pos-cry-P3P6}, \\ & \sum_{1}^{8} Count_{pos-int-P3P4}, \sum_{1}^{8} Count_{pos-int-P3P5}, \sum_{1}^{8} Count_{pos-int-P3P6}, Temperature \Bigg). \end{aligned} \tag{6}$$

From the ML output shown in Tables 1 and 2, the $Uniqueness_{signature}$ yields an accuracy of 89.7%, and the $Position_{signature}$ yields an accuracy of 99.7% when all the features are considered. The impact on accuracy due to the exclusion of one of the features is lesser as compared to Case-1.

5.3.3 Case 3: Accumulation of 8, Two Temperatures. In this case, the accumulated counts at two different temperatures are considered along with the corresponding temperatures. Thus, the $Uniqueness_{signature}$ is a tuple with six features, and the $Position_{signature}$ is a tuple with 14 features.

$$\begin{aligned} Uniqueness_{signature} = & \left(\sum_{1}^{8} Count_{identity-cry}, \sum_{1}^{8} Count_{identity-int}, Temperature \right)_{at\ temperature\ 1}, \\ & \left(\sum_{1}^{8} Count_{identity-cry}, \sum_{1}^{8} Count_{identity-int}, Temperature \right)_{at\ temperature\ 2}; \end{aligned} \tag{7}$$

$$Position_{signature} = \left(\sum_{1}^{8} Count_{pos-cry-P3P4}, \sum_{1}^{8} Count_{pos-cry-P3P5}, \sum_{1}^{8} Count_{pos-cry-P3P6}, \right.$$
$$\left. \sum_{1}^{8} Count_{pos-int-P3P4}, \sum_{1}^{8} Count_{pos-int-P3P5}, \sum_{1}^{8} Count_{pos-int-P3P6}, Temperature \right)_{at\ temperature\ 1},$$
$$\left(\sum_{1}^{8} Count_{pos-cry-P3P4}, \sum_{1}^{8} Count_{pos-cry-P3P5}, \sum_{1}^{8} Count_{pos-cry-P3P6}, \right.$$
$$\left. \sum_{1}^{8} Count_{pos-int-P3P4}, \sum_{1}^{8} Count_{pos-int-P3P5}, \sum_{1}^{8} Count_{pos-int-P3P6}, Temperature \right)_{at\ temperature\ 2}. \quad (8)$$

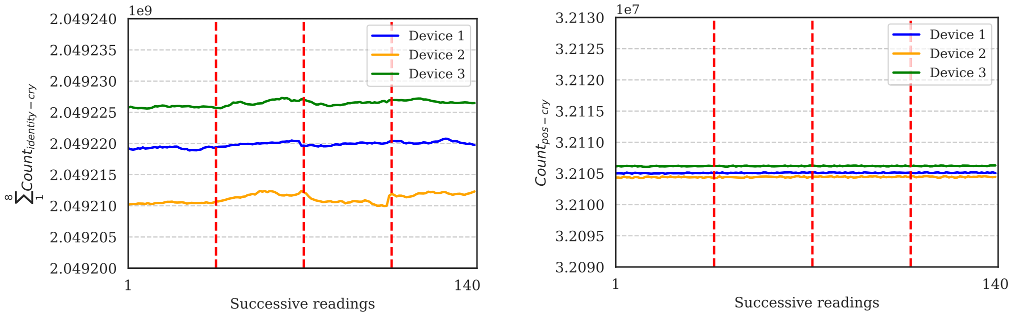
The $Uniqueness_{signature}$ and $Position_{signature}$ at two different temperatures are separated by $6°C - 10°C$. The $Uniqueness_{signature}$ yields an accuracy of 99.4%, and the $Position_{signature}$ yields an accuracy of 99.9% when all the features are considered.

5.3.4 Observations Related to Accuracy. From Tables 1 and 2, we note the following:

(1) The accuracy improves from Case 1 to Case 2 and further to Case 3 for $Uniqueness$ as well as $Position$. Thus, accuracy improves with accumulation. The accuracy further improves when signatures at two distinct temperatures are considered.
(2) For $Uniqueness_{signature}$, we observe that the accuracy is better with $Count_{identity-int}$ as input as compared to $Count_{identity-cry}$. The variation in internal oscillator frequency across devices is higher than the variation in a crystal oscillator. Hence internal oscillator based signature has better distinction across devices.
(3) To achieve an accuracy of greater than 95% for $Uniqueness$, the $Uniqueness_{signature}$ with accumulation at two different temperatures (Case 3) are required.
(4) The $Position_{signature}$ accuracy is 98.5% when all the features are considered, even without accumulation. Hence no accumulation (Case 1) is required for $Position_{signature}$.
(5) The $Position_{signature}$ with $Count_{pos-cry}$ gives better accuracy as compared to $Count_{pos-int}$. The intra-device variation of $Count_{pos-cry}$ is smaller than $Count_{pos-int}$. Hence the crystal-based signatures have better distinction across positions.

5.4 Variation of `Acoustic PUF` with Microphone Sensor

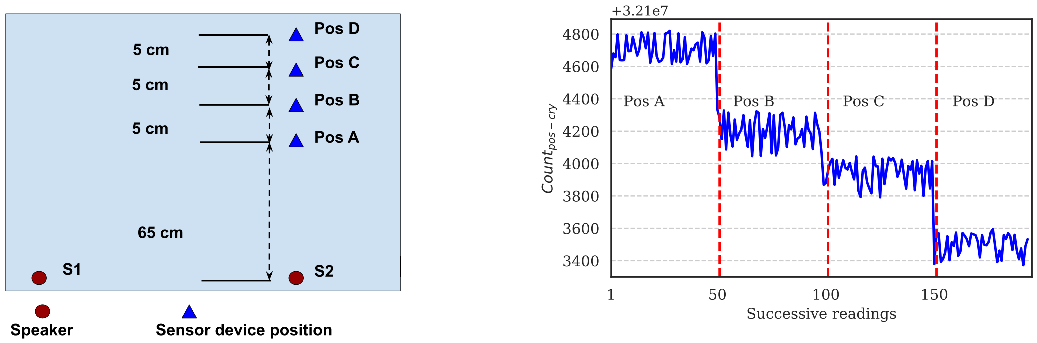
The `Acoustic PUF` should represent the digital core and hence must be independent of the microphone sensor. Figure 12(a) plots the $Uniqueness_{signature}$ for three different devices. Four different microphone devices are used for every device to record the $Uniqueness_{signature}$. The vertical lines in the plot represent the change in the microphone. The standard deviation of the $Uniqueness_{signature}$ across different microphones is within 500 counts. This is comparable to the standard deviation of $Uniqueness_{signature}$ taken through a single microphone. Thus we observe that the $Uniqueness_{signature}$ remain unchanged with a change in microphone. Figure 12(b) plots the $Position_{signature}$ for three devices connected with different microphones kept at the same position. The x-axis represents iterations, and the y-axis represents the $Position_{signature}$. The three lines represent three different devices. The y-axis scale represents $Position_{signature}$ corresponding to 10 cm. We observe that the difference in the $Position_{signature}$ obtained through three microphones is within 0.5 cm. Figure 12 confirms that the microphone sensor has a negligible impact on `Acoustic PUF`.



(a) Variation in $Uniqueness_{signature}$ due to change in microphone

(b) Variation in $Position_{signature}$ due to change in microphone

Fig. 12. Independence of Acoustic PUF with respect to microphone sensor.



(a) Setup to evaluate the sensitivity of $Position_{signature}$

(b) $Position_{signature}$ at different positions

Fig. 13. Setup and plots showcasing the sensitivity of $Position_{signature}$.

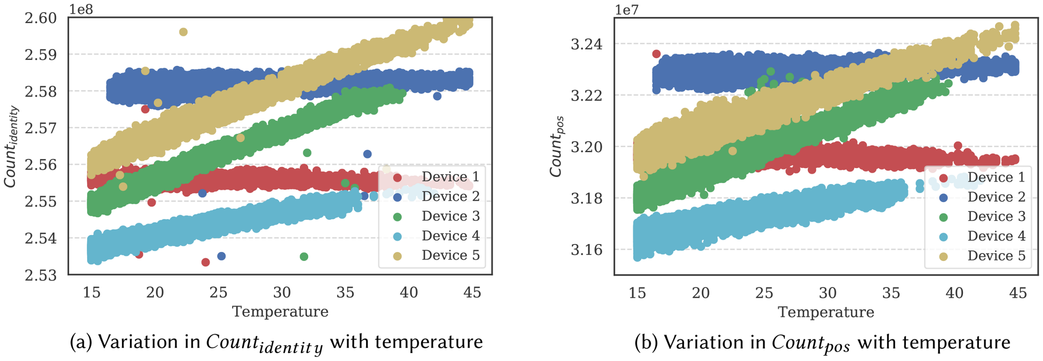
5.5 Sensitivity of Acoustic PUF with Distance

To evaluate the position sensitivity of Acoustic PUF, we experimented by moving the microphone sensor. We assume that the acoustic sources are throughout in fixed positions. Figure 13(a) illustrates one such change; wherein the microphone sensor was moved in increments of 5 cm from position A to positions B, C, and D. Figure 13(b) plots the corresponding signatures. We observe that a displacement of 5 cm is detected through $Position_{signature}$.

5.6 Time and Current Consumption for Acoustic PUF Generation

As shown in Figure 9, the time required for the generation of a single pair of $Count_{identity}$ and $Count_{pos}$ is 25 seconds. Since eight $Count_{identity}$ are accumulated to generate a single $Uniqueness_{signature}$, the latency to generate the first $Uniqueness_{signature}$ is 200 seconds. The subsequent signatures are generated every 25 seconds by accumulating the previous eight $Count_{identity}$. The $Position_{signature}$ is a tuple of multiple $Count_{pos}$, and hence a new value is generated every 25 seconds.

The current consumption during regular device operation for device type D1 as well as device type D2 is 2 mA. We found that the current consumption remains the same during signature generation. Thus Acoustic PUF is generated with negligible current overhead.



(a) Variation in $Count_{identity}$ with temperature

(b) Variation in $Count_{pos}$ with temperature

Fig. 14. Variation in Acoustic PUF with temperature.

5.7 Impact of Temperature Variations on Acoustic PUF

We deployed the sensor devices in an enclosure subjected to variation in ambient temperature from 15°C to 45°C. $Count_{identity}$ and $Count_{pos}$ were recorded along with the corresponding temperatures.

Figures 14(a) and (b) plot the $Count_{identity}$ and the $Count_{pos}$ with respect to temperature for 5 sample devices. The x-axis represents the temperature, and the y-axis represents the corresponding $Count$. We observe that the $Counts$ vary almost linearly with temperature. To account for the variation in $Count_{identity}$ and $Count_{pos}$ with respect to temperature, we measure temperature and provide it as one of the inputs to the ML model. The ML model learns the mappings between the $Counts$ and temperature and hence performs the classification accurately.

Further, the temperature coefficient, i.e., the variations in $Count_{identity}$ and $Count_{pos}$ with respect to temperature are different across devices. The ML model treats the temperature coefficients as additional features when $Uniqueness_{signature}$ and $Postion_{signature}$ at two different temperatures are given to the model. Hence, as observed in Section 5.3, the identification accuracy improves when the $Uniqueness_{signature}$ and $Position_{signature}$ at two different temperatures are considered.

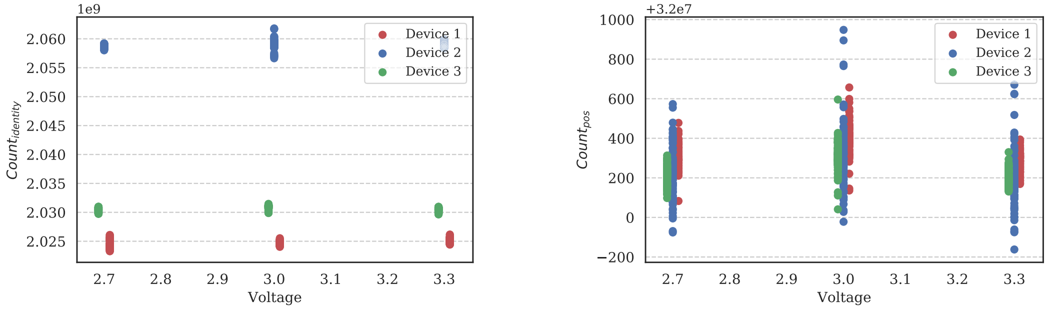
5.8 Impact of Voltage Variations on Acoustic PUF

For three devices, we varied the supply voltage nominally set at 3 V by ±10% to 3.3 V and 2.7 V and noted the corresponding $Count_{identity}$ and $Count_{pos}$. Multiple measurements were taken at each supply voltage. Figures 15(a) and (b) plot the scatter plots of $Count_{identity}$ and $Count_{pos}$ with respect to voltage. The x-axis represents the voltage, and the y-axis represents the corresponding $Count$. We observe that the variations in the $Count_{identity}$ as well as $Count_{pos}$ with respect to voltage, are comparable to the intra-device variations at a single voltage across the measurements. Hence we conclude that $Count_{identity}$ and $Count_{pos}$ are agnostic to variation in supply voltage. The three devices were kept in close proximity causing identical $Count_{pos}$ readings across devices in Figure 15(b).

6 SCALABILITY ANALYSIS FOR ACOUSTIC PUF

In the previous sections, we have shown that deployment of 34 sensor devices creates distinct $Uniqueness_{signature}$. In this section, we show the scalability of $Uniqueness_{signature}$ by evaluating its efficacy for the deployment of thousands of devices.

As the number of devices increases, the likelihood of multiple devices having the same $Uniqueness_{signature}$ for Acoustic PUF also increases. This is due to the fact that the manufacturing variation is bounded. The circuit designs for the real semiconductor parts are the intellectual property of the part manufacturers, and therefore there is difficulty in performing the Monte Carlo simulations to analyse the scalability. Further, it is practically



(a) Variation in $Count_{identity}$ with voltage

(b) Variation in $Count_{pos}$ with voltage

Fig. 15. Variation in `Acoustic PUF` with voltage.

infeasible to evaluate the scalability through the physical deployment of thousands of devices. Hence we perform numerical analysis to check the scalability of $Uniqueness_{signature}$.

Numerical model generation: To create a realistic model, we have extracted the statistical distribution of $Count_{identity}$ from the real-world deployment. Specifically, we have extracted intra-device standard deviation, inter-device standard deviation and the range of temperature coefficients for $Count_{identity-cry}$ and $Count_{identity-int}$. The intra-device standard deviation characterises the distribution of measurements for a single device at a specific temperature. The inter-device standard deviation characterises the distribution of measurements across multiple devices at a specific temperature. The range of temperature coefficients characterises the distribution of temperature coefficients across devices.

We have performed a MATLAB simulation to spawn out multiple devices from the numerical model. For each device, the model generates multiple values over a temperature range of 20°C to 40°C in steps of 0.25°C. At each temperature, 100 readings are generated for every device. The model first generates the mean values of all devices at nominal temperature (30°C) from a normal distribution with the expected value (i.e., 256,000,000) as mean and the inter-device standard deviation. Temperature coefficient for each device is generated through a uniform distribution from the range of observed temperature coefficients. In the next step, the means (across measurements) for every device at each temperature across the temperature range are computed based on the temperature coefficient of the device and the mean at the nominal temperature. Finally, the measurements for all the devices at every temperature is generated through Gaussian distribution using the mean at that temperature and the intra-device standard deviation. This mimics the $Count_{identity-cry}$ and $Count_{identity-int}$ measurements from the actual deployment taken across devices over the temperature range. The $Count_{identity}$ data generated by the MATLAB model is used to compute $Uniqueness_{signature}$ through accumulation.

Numerical model verification: To validate the model, we spawn out 34 devices. The $Uniqueness_{signature}$ data generated by the model for 34 devices is used as input to the Machine Learning classification model. The ML model is a kNN model with $k = 30$, the same as the one used to analyse experimental data in Section 5.3. Three different cases, as discussed in Section 5.3, are considered.

(1) **Case 1:** $Uniqueness_{signature}$ is same as $Count_{identity}$, i.e., no accumulation is done. $Count_{identity}$ at a single temperature is considered as a feature, see Equation (3).
(2) **Case 2:** $Uniqueness_{signature}$ is obtained by accumulating eight $Count_{identity}$. The accumulated $Count_{identity}$ at a single temperature is considered as a feature, see Equation (5).
(3) **Case 3:** $Uniqueness_{signature}$ is obtained by accumulating eight $Count_{identity}$. The accumulated $Count_{identity}$ at two different temperatures are considered as a feature, see Equation (7). The two temperatures are 6°C to 10°C apart.

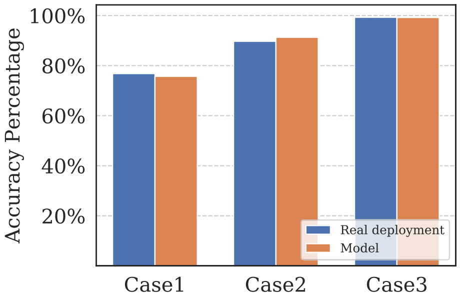


Fig. 16. Comparison of identification accuracy from the real-world deployment with the identification accuracy obtained from model.

The accuracy numbers predicted by the model are 75.7%, 91.3%, and 99.2%. Figure 16 shows that the results are comparable to those obtained from the deployment. This confirms that our numerical model accurately captures the distribution of $Count_{identity}$ from the real-world deployment of devices.

After validating the model, we spawn out 100, 1,000, and 10,000 devices using the model. Multiple values of $Count_{identity}$ for each of the devices across the temperature range of 20°C to 40°C are generated. The generated values are used to train the ML model, and the identification accuracy is checked through 10-fold cross-validation.

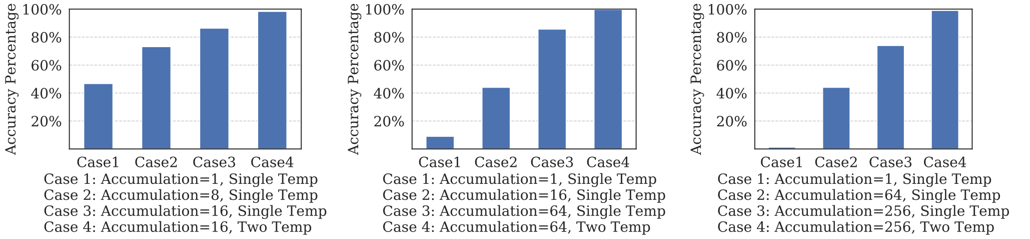
Number of devices = 100: Figure 17(a) shows the identification accuracy for 100 devices for (i) No accumulation, (ii) Accumulation count = 8, (iii) Accumulation count = 16, and (iv) Accumulation count = 16 at two different temperatures. We observe that as the accumulation count increases from 1 to 16, the identification accuracy improves from 46.7% to 86.3%. The accuracy further improves to 98.3% if $Uniqueness_{signature}$ is generated with accumulated counts at two distinct temperatures.

Number of devices = 1,000: As the number of devices increases to 1,000, we observe in Figure 17(b) that higher accumulation is required to achieve the same accuracy. The accuracy is 44% for the accumulation count of 16 (as against 86.3% for 100 devices) and improves to 85.62% for the accumulation count of 64. The accuracy further improves to 99.67% if $Uniqueness_{signature}$ is generated with an accumulation count of 64 at two distinct temperatures.

Number of devices = 10,000: The impact of accumulation for 10,000 devices is shown in Figure 17(c). As the number of devices increases to 10,000, the accuracy is 44% for an accumulation count of 64. The accuracy improves to 73.9% with an accumulation count of 256 and further improves to 99% if $Uniqueness_{signature}$ is generated with an accumulation count of 256 at two distinct temperatures.

Thus we can achieve an identification accuracy of 99% even for 10,000 devices. The increase in accumulation count improves accuracy. The hypothesis is that as the accumulation is increased by N times, the mean of the measurements for $Uniqueness_{signature}$ for a given device is scaled by N times; however, the standard deviation across measurements is scaled by $\sqrt{N}$. This increases the inter-device separation and hence improves the distinction across devices. Initial signature generation requires 256 counts, whereas subsequent generation requires one additional count. Therefore, the time required for `Acoustic PUF` generation remains the same due to successive accumulation across the sliding window. However, the increase in accumulation comes at the expense of increased latency for $Uniqueness_{signature}$. As an example, if 256 counts are accumulated, then the first `Acoustic PUF` would be generated after 256*25 seconds, and thereafter, a new value is generated every 25 seconds.

The accuracy also improves by considering the accumulated count for the devices at different temperatures. The hypothesis is that the devices have different temperature coefficients. Hence, two devices having comparable signatures at one temperature may have distinct signatures at a different temperature. We propose that the device stores intermittent Count and temperature values. While calculating the signature at two different temperatures (as in case 4), any of the earlier stored readings could be used.



(a) Variation in accuracy for 100 devices (b) Variation in accuracy for 1000 devices (c) Variation in accuracy for 10000 devices

Fig. 17. Variation in identification accuracy with respect to accumulation count.

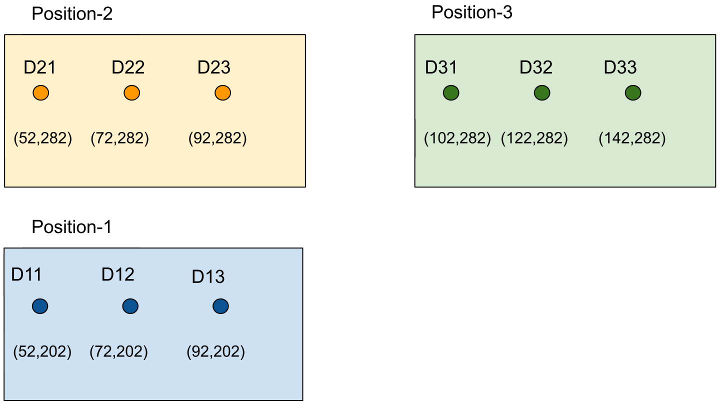


Fig. 18. Setup for tuning the sensitivity of $Position_{signature}$.

7 DISCUSSION AND FUTURE WORK

- $Uniqueness_{signature}$: The uniqueness of identity signature holds the promise that the inspected component at a manufacturing facility is the same as the one being delivered and integrated into the production workflow. We have shown that the Acoustic PUF based identity not only scales to thousands of devices but also remains invariant to the ambient conditions and support hardware such as microphones. The architected solution is generic enough to support any custom or commercial embedded devices.
- $Position_{signature}$: The results related to the $Position_{signature}$ as discussed in Section 5, assumes that the number and the position of acoustic sources are fixed, and it could be argued that the signatures would vary if these sources are moved. Such a change in their position could be trivially identified by a simultaneous change in $Position_{signature}$ of all the sensor devices. Further, the sensitivity of the $Position_{signature}$ discussed in Section 5.5, as well as its range, could be enhanced by carefully selecting the number of acoustic sources and placing them appropriately. On the contrary, if the application is such that a slight change in position of devices is expected during the normal functionality, then the sensitivity of $Position_{signature}$ could be tuned. In such applications, collecting data to encompass the real-world displacements for training the model will serve the purpose. As an example, we collected $Count_{pos}$ by displacing three devices kept at three different positions. Each device was moved across three places, together considered as data for the same position, as shown in Figure 18. Six hundred data points were collected for each position. The ML model was trained with $Count_{pos}$ values across the places. We observed that the accuracy of detecting positions stays greater than 99%. The $Position_{signature}$ could be leveraged independent of the

$Uniqueness_{signature}$ during a maintenance schedule to identify the displacement of installed sensor devices as discussed in Section 2.

- *Impact of Multipath*: The repeatability of signatures, as discussed in Sections 5.1 and 5.2, depends upon the path between acoustic sources and the microphone. The experiments were conducted indoors, where the sensor devices would experience multipath reception due to several reflecting surfaces. Thus, we believe that our solution is agnostic to the presence of multipath.
- *Similarity to Localisation*: The method of generating $Position_{signature}$ as discussed in Section 3.2, although appears similar to the TDOA [19, 34] localisation technique, the goal is to identify the change in position rather than localising the sensor device. Thus, it differs from localisation in the following manner: (a) The native clock count and its associated precision are exploited. (b) The difference in the clock counts generated from the two tones is used as the $Position_{signature}$. Therefore, while $Position_{signature}$ requires output in terms of the difference in clock count for the purpose of fingerprinting, TDOA directly uses the time difference output. (c) Further, our methodology uniquely combines the device identity information along with $Position_{signature}$ to create a robust `Acoustic PUF`.

8 LIMITATIONS AND MITIGATION

8.1 Ageing

The experiments discussed in Section 5 were conducted for a duration of 15 days over three months and later resumed after a break of two months. We did not observe any significant difference between the batch of readings collected before and after the break. To further understand the impact of ageing, we compared two datasets collected one year apart. The devices were inactive during the intermediate duration. The data was collected for six sample devices for a duration of one week. We used the old dataset for training a kNN model and verified the accuracy by using the new dataset as test data. The accuracy was 93%, which is comparable with the accuracy when the same dataset was used for training and testing with a 50%–50% split.

However, it is unclear from the results whether there is any gradual change in signatures caused by drift in component values due to ageing over a longer duration. Accelerated life tests must be conducted to confirm the ageing drift.

Analysis and Mitigation: In the event of an ageing drift, we propose the following mitigation mechanisms. In our proposed system, the number of clock ticks between the audio pulses are counted to generate the signatures. Thus, signature ageing depends primarily upon the ageing of the oscillators. The oscillators may be (i) on-chip crystal oscillators, where the internal active circuit is connected to the external crystal, (ii) precise external oscillators, and (iii) internal oscillators.

Typically, an on-chip crystal oscillator with an external crystal is used. A high precision, highly stable external crystal could be connected with the active circuit internal to the controller. While the typical ageing drift for the crystal is in the range of 1–2 ppm/year [27], highly stable crystals with ageing less than 0.5 ppb/day are available [29]. Such a crystal could be integrated into a highly stable oscillator. Alternatively, precise external oscillators like high stability crystal oscillators with 125-ppb change over 2.25 years are available and could be used [28].

For our application, we propose an oscillator with a drift of 0.1ppm/year ageing. As discussed in Section 2.5, with a 16-MHz crystal oscillator and 16-second duration between the pulses, we expect a pulse count of 256,000,000. A crystal oscillator with an ageing specification of +/- 0.1 ppm/year would change the pulse count by merely 26 pulse counts. From Figure 2, we see that the standard deviation for successive pulse counts is in the range of 100 counts. Thus, a change of +/-26 pulse counts due to ageing will have minimal impact on signatures from our PUF. A recalibration every two years might be sufficient to account for ageing. Further, if the inter-device variation between the devices is "sufficient," then the change due to ageing drift may not cause a misidentification of devices. Thus, the recalibration duration could be proportionately extended.

The ageing phenomenon for the internal oscillator is not well studied and is expected to depend upon the specific circuit implementation in the silicon. However, the corresponding standard deviation for successive counts for the internal oscillator in our device is in the range of 70,000 counts, thus around 700 times more than the crystal oscillator. We believe that a similar recalibration might be sufficient for the internal oscillator.

We could further complement the hardware approach through machine learning techniques. In the ML context, if the statistical properties of the target variable (device ID in our case) gradually change with time, then it is known as concept drift [49]. Concept drift is a well-studied phenomenon, and newer techniques like incremental learning are emerging to address concept drift [50]. Concept drift and incremental learning could be further studied and adopted to address the ageing degradation for PUF.

9 RELATED WORK

Multiple approaches have been suggested in the literature for the generation of the identity of an embedded sensor device. For a device connected over a network, signature analysis and behaviour profiling of protocols have been implemented. IoT Sentinel [30] and ProfilIoT [26] propose extracting features across different protocol layers. The work in Reference [2] uses temporal properties by extracting inter-arrival time between consecutive packets and applying deep learning for the classification of devices. While these approaches successfully identify a class of devices, they fail to perform identification at the device instance level.

For identification at the device instance level, storage of unique identity in the non-volatile memory has been one of the practised approaches. However, identity thefts have been reported for this approach. The identity could be stolen through scanning electron microscopy [10] or altered through fault injection attacks [38]. Approaches like tagging the devices through plant DNA [45] or usage of dielets [33] during the manufacturing of devices have been proposed to secure the identity. However, these approaches are expensive and impossible to implement for systems created from commercially off the shelf devices.

For device instance level identification, PUFs have been studied widely [22, 36]. Different variants of Ring oscillator PUF [1, 25, 42] use the difference in RO frequencies for the generation of signatures. Arbiter PUF [24] uses the variation in delay paths. Custom analog circuits exploit the mismatch in differential pairs [15] and comparator offsets [8] for generating signatures. These PUFs need a custom circuit implementation. The memory PUF [20] uses the startup values of RAM as a signature. However, the generation of signatures demand power cycling and hence are invasive. The usage of offset for ADC-DAC combination has been proposed as PUF in Reference [16]. This PUF requires DAC for implementation. Fingerprinting of devices through acoustic means have been based on the anomalies introduced by the microphone while recording the sound [12, 52]. However, these approaches fingerprint the sensor rather than the digital core.

Sensor device position is widely studied from a localisation perspective [40]. The existing literature suggests several methods for sound source localisation. The approaches include the Received Signal Strength approach, **Time of Arrival (TOA)**, TDOA [9]. Localisation of microphones using sound sources at known locations has been discussed in References [18, 19, 48]. The proposed approaches primarily rely on a combination of TOA and TDOA methods. We have adapted the TDOAs native clock count approach, included signature profiling and combined the device signature to create a unique device identity together with position.

10 CONCLUSION

In this article, we presented a novel way to secure the identification of sensor devices and thus facilitated supply-chain traceability from manufacturing facility to deployment. We proposed `Acoustic PUF`, which combines the identity component and the position component, creating a strong signature. `Acoustic PUF` is derived from the innate properties of sensor nodes and is hence unclonable. Our `Acoustic PUF` does not require custom circuits. Our experimental evaluation and simulations have shown that `Acoustic PUF` is a scalable and promising alternative to generate a hardware root of trust.

ACKNOWLEDGMENTS

The authors are thankful to the reviewers of the journal for their insightful comments.

REFERENCES

[1] Emrah Abtioglu, Ramazan Yeniçeri, Burak Gövem, Emre Göncü, Müstak E. Yalçin, and Gökay Saldamli. 2017. Partially reconfigurable IP protection system with ring oscillator based physically unclonable functions. In *Proceedings of the New Generation of Circuits and Systems Conference (NGCAS'17)*. IEEE, 65–68.

[2] Sandhya Aneja, Nagender Aneja, and Md Shohidul Islam. 2018. IoT device fingerprint using deep learning. In *Proceedings of the IEEE International Conference on Internet of Things and Intelligence System (IOTAIS'18)*. IEEE, Bali,Indonesia, 174–179.

[3] Kristina Armstrong, Sujit Das, and Joe Cresko. 2020. The energy footprint of automotive electronic sensors. *Sustain. Mater. Technol.* 25 (2020), e00195. https://doi.org/10.1016/j.susmat.2020.e00195

[4] Aircraft Electronics Association. 2019. AEA Unveils Third-quarter 2019 Avionics Market Report. Retrieved from https://aea.net/newsitem.asp?ID=2965.

[5] Rameshkumar Balasubramanian. 2017. Aircraft overhead bin monitoring and alert system. (Aug. 29 2017). US Patent 9,745,064.

[6] Beamex. *Why Calibrate? Reasons for Calibration*. Technical Report. Retrieved from http://cdn2.hubspot.net/hubfs/2203666/Beamex_White_Papers/Beamex_White_Paper_-_Why_calibrate_-Reason_for_calibration_ENG.pdf.

[7] Erik Blasch, Paul Kostek, Pavel Pačes, and Kathleen Kramer. 2015. Summary of avionics technologies. *IEEE Aerospace and Electronic Systems Magazine* 30, 9 (2015), 6–11. Retrieved from https://10.1109/MAES.2015.150012.

[8] Troy Bryant, Sreeja Chowdhury, Domenic Forte, Mark Tehranipoor, and Nima Maghari. 2016. A stochastic approach to analog physical unclonable function. In *Proceedings of the IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS'16)*. IEEE, 1–4.

[9] Maximo Cobos, Fabio Antonacci, Anastasios Alexandridis, Athanasios Mouchtaris, and Bowon Lee. 2017. A Survey of Sound Source Localization Methods in Wireless Acoustic Sensor Networks. *Wireless Communications and Mobile Computing*. Article ID (2017) 3956282, 24 pages. Retrieved from https://doi.org/10.1155/2017/3956282

[10] Franck Courbon, Sergei Skorobogatov, and Christopher Woods. 2017. Reverse engineering flash EEPROM memories using scanning electron microscopy. In *Smart Card Research and Advanced Applications*, Kerstin Lemke-Rust and Michael Tunstall (Eds.). Lecture Notes in Computer Science, vol 10146, Springer International Publishing, Cham. Retrieved from https://doi.org/10.1007/978-3-319-54669-8_4

[11] Cypress semiconductors 2018. *PSoC 63 with BLE Architecture Technical Reference Manual, Document No. 002-18176*.

[12] Anupam Das, Nikita Borisov, and Matthew Caesar. 2014. Do you hear what i hear? Fingerprinting smart devices through embedded acoustic components. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS'14)*. Association for Computing Machinery, New York, NY, 441–452. https://doi.org/10.1145/2660267.2660325

[13] Analog Devices. 2020. LTspice. Retrieved December 2019 from https://www.analog.com/en/design-center/design-tools-and-calculators/ltspice-simulator.html.

[14] Analog Devices. 2020. LTspice: Worst-Case Circuit Analysis with Minimal Simulations Runs. Retrieved from https://www.analog.com/en/technical-articles/ltspice-worst-case-circuit-analysis-with-minimal-simulations-runs.html.

[15] Sabyasachi Deyati, Barry Muldrey, Adit Singh, and Abhijit Chatterjee. 2017. Design of efficient analog physically unclonable functions using alternative test principles. In *Proceedings of the InternationalMixed Signals Testing Workshop (IMSTW'17)*. IEEE, 1–4.

[16] Adam Duncan, Lei Jiang, and Martin Swany. 2018. Repurposing SoC analog circuitry for additional COTS hardware security. In *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST'18)*. IEEE, 201–204.

[17] M. Ford and J. D. Triggs. 2006. Traceability requirements in electronics assembly. In *Intelligent Production Machines and Systems*, D. T. Pham, E. E. Eldukhri, and A. J. Soroka (Eds.). Elsevier Science Ltd, Oxford, 656–662. https://doi.org/10.1016/B978-008045157-2/50114-0

[18] Diego B. Haddad, Wallace A. Martins, Mauricio do V. M. Da Costa, Luiz W. P. Biscainho, Leonardo O. Nunes, and Bowon Lee. 2015. Robust acoustic self-localization of mobile devices. *IEEE Trans. Mobile Comput.* 15, 4 (2015), 982–995.

[19] Diego B. Haddad, Leonardo O. Nunes, Wallace A. Martins, Luiz W. P. Biscainho, and Bowon Lee. 2013. Closed-form solutions for robust acoustic sensor localization. In *Proceedings of the IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*. IEEE, 1–4.

[20] Daniel E. Holcomb, Wayne P. Burleson, Kevin Fu, et al. 2007. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In *Proceedings of the Conference on RFID Security*, Vol. 7. 01.

[21] Invensense. 2016. *Invensense 40618-v1.0 Datasheet*. Invensense.

[22] Shital Joshi, Saraju P. Mohanty, and Elias Kougianos. 2017. Everything you wanted to know about PUFs. *IEEE Potentials* 36, 6 (2017), 38–46.

[23] Ashish Kumar, Saurabh Goyal, and Manik Varma. 2017. Resource-efficient machine learning in 2 KB RAM for the internet of things. In *Proceedings of the 34th International Conference on Machine Learning (Proceedings of Machine Learning Research)*, Doina Precup and Yee Whye Teh (Eds.), Vol. 70. PMLR, 1935–1944.

[24] Jae W. Lee, Daihyun Lim, Blaise Gassend, G. Edward Suh, Marten Van Dijk, and Srinivas Devadas. 2004. A technique to build a secret key in integrated circuits for identification and authentication applications. In *Proceedings of the Symposium on VLSI Circuits Digest of Technical Papers*. IEEE, 176–179.

[25] Cédric Marchand, Lilian Bossuet, Ugo Mureddu, Nathalie Bochard, Abdelkarim Cherkaoui, and Viktor Fischer. 2018. Implementation and characterization of a physical unclonable function for IoT: A case study with the TERO-PUF. *IEEE Trans. Comput.-Aid. Des. Integr. Circ. Syst.* 37, 1 (2018), 97–109.

[26] Yair Meidan, Michael Bohadana, Asaf Shabtai, Juan David Guarnizo, Martín Ochoa, Nils Ole Tippenhauer, and Yuval Elovici. 2017. ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In *Proceedings of the Symposium on Applied Computing (SAC'17)*. Association for Computing Machinery, New York, USA, 506–509. https://doi.org/10.1145/3019612.3019878

[27] Microchip. Vectron Product Portfolio. Retrieved February 2021 from https://www.vectron.com/products/crystals/precision_crystals_index.htm.

[28] Microchip. VT-803 Temperature Compensated Crystal Oscillator. Retrieved February 2021 from https://www.vectron.com/products/tcxo/vt-803.pdf.

[29] Microchip. XR-U Crystal Resonator. Retrieved February 2021 from https://www.vectron.com/products/hitemp/XR-U_HC37_TO8_Release_1.pdf.

[30] Markus Miettinen, Samuel Marchal, Ibbad Hafeez, N. Asokan, Ahmad-Reza Sadeghi, and Sasu Tarkoma. 2017. IoT Sentinel: Automated device-type identification for security enforcement in IoT. In *Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS'17)*. IEEE, 2177–2184.

[31] Nordic Semiconductors 2017. *nRF52832—Product Specification v1.0*. Retrieved December 2019 from https://infocenter.nordicsemi.com/pdf/nRF52832_PS_v1.0.pdf.

[32] Nordic Semiconductors 2019. *nRF52840—Product Specification v1.1*. Retrieved January 2020 from https://infocenter.nordicsemi.com/pdf/nRF52840_PS_v1.1.pdf.

[33] Parrish Ralston, David Fry, Scott Suko, Bryce Winters, Matthew King, and Robert Kober. 2016. Defeating counterfeiters with microscopic dielets embedded in electronic components. *Computer* 49, 8 (2016), 18–26.

[34] Vikas C. Raykar, Igor V. Kozintsev, and Rainer Lienhart. 2004. Position calibration of microphones and loudspeakers in distributed computing platforms. *IEEE Trans. Speech Aud. Process.* 13, 1 (2004), 70–83.

[35] A. Rouse and T. Marshall. 2001. The extent and implications of sphygmomanometer calibration error in primary care. *J. Hum. Hypertens.* 15, 9 (2001), 587–591.

[36] Ulrich Rührmair and Daniel E. Holcomb. 2014. PUFs at a glance. In *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE'14)*. IEEE, Dresden, Germany, 1–6.

[37] Sukhpal Singh Sandhu, Sandip Chattopadhyay, Michael Kevin Birch, and Neeta Ray-Chaudhuri. 2005. Frequency of goldmann applanation tonometer calibration error checks. *J. Glaucoma* 14, 3 (2005), 215–218.

[38] Jörn-Marc Schmidt, Michael Hutter, and Thomas Plos. 2009. Optical fault attacks on AES: A threat in violet. In *Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC'09)*. IEEE, 13–22.

[39] Nordic Semiconductors. nRF52 DK. Retrieved December 2019 from https://www.nordicsemi.com/Software-and-Tools/Development-Kits/nRF52-DK.

[40] Rathin Chandra Shit, Suraj Sharma, Deepak Puthal, and Albert Y Zomaya. 2018. Location of things (LoT): A review and taxonomy of sensors localization in IoT infrastructure. *IEEE Commun. Surv. Tutor.* 20, 3 (2018), 2028–2061.

[41] Richard K. Simms, Stephen G. Dame, Mark L. Cloud, and Todd D. Smith. 2020. Vehicle stowage bin assemblies having weight sensors. (May 12 2020). US Patent 10,647,429.

[42] G. Edward Suh and Srinivas Devadas. 2007. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th ACM/IEEE Design Automation Conference (DAC'07)*. IEEE, 9–14.

[43] K. M. Talluru, V. Kulandaivelu, N. Hutchins, and I. Marusic. 2014. A calibration technique to correct sensor drift issues in hot-wire anemometry. *Meas. Sci. Technol.* 25, 10 (2014), 105304.

[44] Fatemeh Tehranipoor, Nima Karimian, Wei Yan, and John A Chandy. 2017. DRAM-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Trans. VLSI Syst.* 25, 3 (2017), 1085–1097.

[45] Mark M. Tehranipoor, Ujjwal Guin, and Swarup Bhunia. 2017. Invasion of the hardware snatchers. *IEEE Spectr.* 54, 5 (2017), 36–41.

[46] J. P. Trovao. 2019. Trends in automotive electronics [Automotive Electronics]. *IEEE Vehic. Technol. Mag.* 14, 4 (2019), 100–109.

[47] Girish Vaidya, Akshay Nambi, TV Prabhakar, Suhas Sudhakara, et al. 2020. IoT-ID: A novel device-specific identifier based on unique hardware fingerprints. In *Proceedings of the IEEE/ACM 5th International Conference on Internet-of-Things Design and Implementation (IoTDI'20)*. IEEE, 189–202.

[48] Lin Wang, Tsz-Kin Hon, Joshua D. Reiss, and Andrea Cavallaro. 2015. Self-localization of ad-hoc arrays using time difference of arrivals. *IEEE Trans. Sign. Process.* 64, 4 (2015), 1018–1033.

[49] Wikipedia. Concept Drift. Retrieved February 2021 from https://en.wikipedia.org/wiki/Concept_drift.

[50] Wikipedia. Incremental (Online) Learning with Scikit-Multiflow. Retrieved February 2021 from https://towardsdatascience.com/incremental-online-learning-with-scikit-multiflow-6b846913a50b.

[51] Wikipedia. 2019. Ring Oscillator. Retrieved January 2020 from https://en.wikipedia.org/wiki/Ring_oscillator/.

[52] Zhe Zhou, Wenrui Diao, Xiangyu Liu, and Kehuan Zhang. 2014. Acoustic fingerprinting revisited: Generate stable device ID stealthily with inaudible sound. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS'14)*. Association for Computing Machinery, New York, NY, 429–440. https://doi.org/10.1145/2660267.2660300

Received 30 August 2020; revised 10 July 2021; accepted 23 September 2021