MAG-PUF: Magnetic Physical Unclonable Functions for Device Authentication in the IoT

Omar Adel Ibrahim[1(✉)], Savio Sciancalepore[2,3], and Roberto Di Pietro[1]

[1] College of Science and Engineering (CSE), Information and Computing Technology (ICT) Division, Hamad Bin Khalifa University (HBKU), Doha, Qatar
{oaibrahim,rdipietro}@hbku.edu.qa

[2] Department of Mathematics and Computer Science, Eindhoven University of Technology (TU/e), Eindhoven, The Netherlands
s.sciancalepore@tue.nl

[3] Eindhoven Artificial Intelligence Systems Institute (EAISI), Eindhoven, The Netherlands

Abstract. Authenticating Internet of Things (IoT) devices is still a challenge, especially in deployments involving low-cost constrained nodes. The cited class of IoT devices hardly support dynamic re-keying solutions, hence being vulnerable to several attacks. To provide a viable general-purpose solution, in this paper we propose MAG-PUF, a novel lightweight authentication scheme based on the usage of unintentional magnetic emissions generated by IoT devices as Physical Unclonable Functions (PUFs). Specifically, through MAG-PUF, we collect unintentional magnetic emissions produced by the IoT devices at run-time while executing pre-defined reference functions, and we verify the match of such emissions with the profiles collected at enrolment time, providing device authentication. MAG-PUF enjoys unique flexibility, allowing the selection of an unlimited number and types of reference functions. We extensively assessed the performance of MAG-PUF through experiments on 25 Arduino devices and a set of exemplary reference functions. We obtained an authentication accuracy above 99%, hence proving the feasibility of using code-driven magnetic emissions as a lightweight, efficient, and robust PUF for IoT devices.

Keywords: Magnetic emissions · PUF · Authentication · IoT

1 Introduction

Internet of Things (IoT) devices are nowadays increasingly deployed in homes, offices, medical, electricity, and transportation domains, to name a few [41], with an installed base of a few billions, and counting [42]. Unfortunately, as acknowledged by several reports [39], security issues are still one of the most critical

F. Li et al. (Eds.): SecureComm 2022, LNICST 462, pp. 130–149, 2023.
https://doi.org/10.1007/978-3-031-25538-0_8

concerns, preventing the unleashing of the full potential behind the IoT. On the one hand, IoT devices often find applications in natively-insecure environments, being the ideal target of various attacks. On the other hand, such devices are usually so constrained in their processing, memory, and energy resources that they cannot support Public Key Infrastructure (PKI) at all, and sometimes even the usage of symmetric key cryptography techniques might significantly affect their lifetime and usability [34]. Moreover, when symmetric cryptography operations are supported, several devices use hard-coded cryptography materials. However, due to the simple design of the devices and the unattended nature of many IoT deployments, attackers can capture the devices and easily recover such keys, fully compromising them [7].

To address the above-described issues, Physical Unclonable Functions (PUFs) have been proposed as a viable and effective alternative [28] to authenticate devices. In a nutshell, PUFs leverage the finding that, despite Integrated Circuits (ICs) are assembled in a precise fabrication process, unintentional variations always occur at the sub-micrometer level, causing any two ICs to be never exactly identical. PUFs take into account such unique properties of any specific device, allowing to generate lightweight chip-dependent unique signatures, that are almost impossible to reproduce either synthetically or by using other devices [46]. Thus, when applied appropriately in the IoT domain, PUFs can efficiently and effectively bypass the need for both complex cryptography operations and hard-coded secrets, allowing system administrators to authenticate IoT devices at low-cost [40].

Despite the above introduced advantages, PUFs are still hardly usable in the IoT context. Indeed, many of the schemes proposed in the literature leverage unique properties of specific memory modules and low-layer circuits, difficult to generalize and to use in low-cost general-purpose IoT devices. Other solutions, such as the ones based on RF emissions, usually do not scale well for large deployments, providing limited security guarantees (see Sect. 5 for more details).

Contribution. In this paper, we design *MAG-PUF*, a novel and lightweight scheme exploiting the unique randomness of unintentional magnetic emissions produced by IoT devices when computing a function to generate Physical Unclonable Functions. Specifically, deploying *MAG-PUF*, the IoT system owner can select a theoretically-unlimited number of reference functions to be used for authentication purposes. The profile of the unintentional magnetic emissions radiated by the devices when executing the reference functions is first acquired at enrolment time, and then checked for consistency at run-time. To this aim, as a novel building block in the PUF area, *MAG-PUF* features Machine Learning (ML)-based classification tools, used to model the magnetic emissions and check for the match of a specific acquisition with the expected profile. Our extensive experimental performance assessment, performed considering 25 Arduino IoT devices and a set of exemplary reference functions, reported a remarkable classification accuracy of above 99%, as well as PUF-related metrics very close to the optimal ones (Intra-PUF Distance of 0.02 and Inter-PUF Distance of 0.51).

Overall, thanks to the customized usage of near-field magnetic emissions and the integration of ML tools, *MAG-PUF* emerges as a novel, lightweight, and secure primitive for authenticating constrained IoT devices, natively offering scalability and robustness features for safety-critical IoT deployments.

Roadmap. This paper is organized as follows: Sect. 2 describes the scenario; Sect. 3 describes *MAG-PUF* in details; Sect. 4 reports an extensive performance assessment and highlights further research directions; Sect. 5 reviews related work; and, finally, Sect. 6 concludes the paper and outlines future work.

2 Scenario, Use-Cases, and Requirements

In this section, we introduce our considered scenarios, assumptions and the considered requirements.

2.1 Scenario and Assumptions

We consider a generic IoT network, i.e., a ubiquitous ecosystem where devices communicate and exchange information without the need for human intervention [3]. Our solution is also built on some realistic assumptions. First, we assume that the IoT devices are resource-constrained in terms of memory and energy. As a result, they cannot use a PKI, because of the overwhelming computational cost. Also, we consider a network where the IoT devices do not have specific tools or capabilities, such as ML-based functionalities or Software-defined radio (SDR) capabilities. Conversely, the devices rely on external equipment to collect and process their unintentional magnetic emissions (either the *PUF Manager* or the *verifier*, see below). The IoT devices in the network can be connected with each other or directly with a central network manager using either a wired or wireless interface, depending on the specific deployment, setup, and security requirements.

From the security perspective, we aim to provide physical-layer authentication of the IoT devices. Indeed, not featuring PKI-based solutions, the IoT devices should be able to prove their identity leveraging features (e.g., non-idealities) available at the physical-layer. In our work, we aim to reach the aforementioned objective by establishing a PUF-based challenge-response pairs (CRP) database (in a form of a trained ML model), utilizing random reference functions and their unintentional magnetic emissions to authenticate the devices.

2.2 Adversary Model

We consider a powerful adversary, namely, $\mathcal{A}$, characterized by both passive and active capabilities. We assume $\mathcal{A}$ has access to a much more powerful equipment than the deployed IoT devices, not characterized by any energy or processing limitations. Also, $\mathcal{A}$ could use advanced wireless reception tools, such as directional antennas, to boost its reception capabilities. We also consider an omnipresent

adversary, present in the field before, during, and after the deployment of the IoT devices. Overall, $\mathcal{A}$ aims to authenticate itself as a legitimate node in the deployed IoT network, in place of a target IoT device. To this aim, we assume $\mathcal{A}$ can mimic other devices' messages, initiate a session, eavesdrop packets, and replay captured messages. In this context, the objective of (*MAG-PUF*) is to thwart such an adversary by providing physical-layer authentication of the IoT devices in the network.

2.3 Requirements

PUF-based solutions conceived to provide authentication of the IoT devices has to fulfill several requirements, outlined below [24].

- *Constructibility*: A PUF class $\mathbb{P}$ is said to be constructible if it is possible to produce a random *puf* instance by invoking a specific *Create* function: $puf \leftarrow \mathbb{P}$.Create.
- *Evaluability*: A PUF class $\mathbb{P}$ is said to be evaluable if it is constructible and it is possible to evaluate a response y for any random PUF instance $puf \in \mathbb{P}$ and any random challenge $x \in \mathbb{X}$: $y \leftarrow puf(x).Eval$.
- *Reproducibility*: A PUF class $\mathbb{P}$ is said to be reproducible if it is evaluable, and the probability of the *Intra-PUF Distance* being small is high. The *Intra-PUF Distance* is defined as the difference between two separate evaluations (responses) of the same challenge produced by the same device, preferably averaging values close to 0.
- *Uniqueness*: A PUF class $\mathbb{P}$ is said to exhibit uniqueness if it is evaluable, and the probability of the *Inter-PUF Distance* being large is high. The *Inter-PUF Distance* is defined as the difference between two separate evaluations (responses) of the same challenge produced by different devices, preferably averaging values close to 0.5.
- *Identifiability*: A PUF class $\mathbb{P}$ is said to be identifiable if it is reproducible and unique, and the probability that *Inter-PUF Distance* being greater than the *Intra-PUF Distance* is high.

In Sect. 4.2, we will prove the conformity of *MAG-PUF* with all the cited requirements.

3 Proposed Framework

In this section, we provide the details of *MAG-PUF*, our solution to provide authentication of energy-constrained IoT devices via magnetic-based PUFs.

3.1 *MAG-PUF* in a Nutshell

Figure 1 provides an overview of our proposed solution. Overall, *MAG-PUF* allows a verifier (e.g., the local system administrator or another system/device on

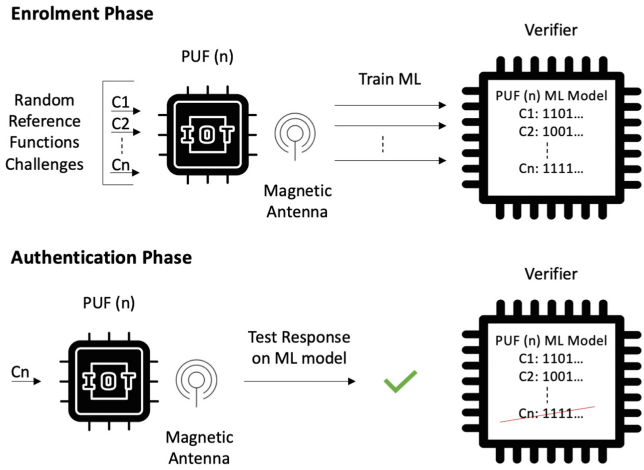


Fig. 1. Overview of *MAG-PUF*.

its behalf) to authenticate a prover (an IoT device), through the analysis of the profile of the unintentional magnetic emissions generated by the prover during the execution of a *reference function*, i.e., a sequence of operations appropriately selected by the verifier.

In brief, *MAG-PUF* consists of two phases, i.e., the *enrolment Phase* and the *Authentication Phase*. The former is executed upon manufacture, by: (i) supplying several *reference functions* to the prover; (ii) extracting the corresponding unintentional magnetic emissions generated by the device; and, (iii) creating the corresponding *reference models*, via ML algorithms. At run-time, when the system administrator or any other entity (namely, the verifier) requires authentication of the IoT device(s), it randomly chooses one or more of the available *reference functions*, it captures the corresponding unintentional magnetic emissions, and it checks if the corresponding real-time profile of the unintentional magnetic emissions matches the one available for the prover, via ML-based classification tools. If there is a match, the prover IoT device is authenticated successfully; otherwise, authentication fails.

3.2 Actors

Overall, *MAG-PUF* involves the following three entities.

- *Prover*. It is an IoT device, to be deployed in a specific scenario. We do not make any assumption for this device, besides the integration of communication capabilities to interact with other systems (PUF Manager) or devices (verifier).
- *PUF Manager*. It is a local entity, managed by a specific system administrator. Its role is manifold: (i) deciding on a set of *reference functions*; (ii) running them on the prover before the deployment; (iii) acquiring the corresponding

unintentional magnetic emissions; (iv) generating their profile, via ML-based tools; (v) storing such profiles on a dedicated server; and, finally, (vi) making them available to the verifier. Thus, we assume it is equipped with the tools necessary to acquire magnetic emissions, such as magnetic antennas, and signal analysis tools (e.g., SDR).

– *Verifier.* It is a remote system or device, interested in authenticating the prover. To this aim, it interacts both with the prover, to acquire its run-time unintentional magnetic emissions, and with the PUF Manager, to download the profile of the unintended magnetic emissions of the prover and the specific reference function submitted to the prover. Similar to the PUF Manager, the verifier also features tools to acquire magnetic emissions and run signal analysis.

3.3 Modules

MAG-PUF relies on four modules, described below.

– **Emissions Extraction Module.** This module, installed on the PUF manager and the verifier, is responsible for recording the unintentional magnetic emissions generated from specific IoT devices when executing particular reference functions. The collected raw data of magnetic emissions include: (i) timestamp, in msec; (ii) acquisition frequency, in Hz; and, (iii) value of the Received Signal Strength (RSS), in dBm. The collected data are provided as input to the *Features Extraction Module*.

– **Features Extraction Module.** This module, installed on the PUF Manager and on the verifier, is responsible for extracting the relevant features from the data collected by the Emissions Extraction Module. It operates in three stages, i.e., *Data Normalization*, *Regions Definitions*, and *Features Computation*.

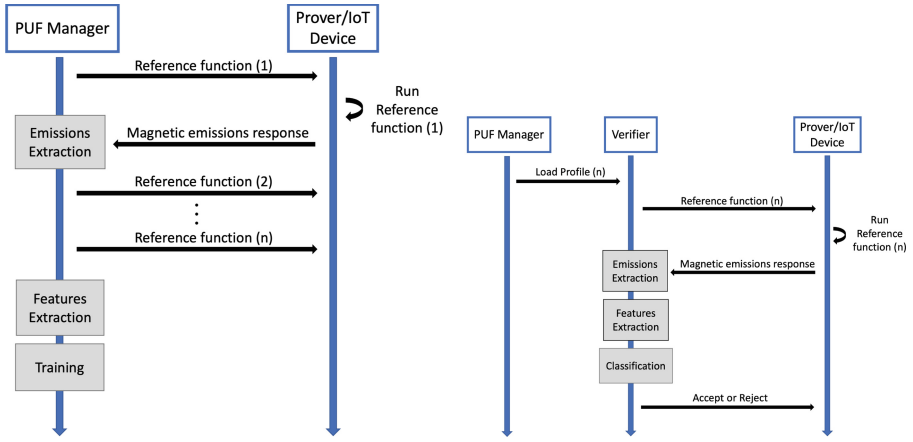
- **Data Normalization**. We first normalize the magnetic emissions power spectral density readings recorded in dBm to the range $[0 \dots 1]$. Specifically, assuming that x_i is a sample of the readings, and X_{MIN} and X_{MAX} are the minimum and the maximum value of the readings, the normalized sample $\hat{x_i}$ is calculated as: $\hat{x_i} = \frac{x_i - X_{MIN}}{(X_{MAX} - X_{MIN})}$. This step is important to allow for cross-comparison between different recordings, by eliminating small differences in the measured power levels due to minor misalignment of the measurement setup.
- **Regions Definition**. In the collected data, each sample of magnetic emissions power level in dBm is associated with a specific timestamp and frequency. In this step, we divide each trace of magnetic emissions into a specific number of regions, with each region comprising the power level readings collected at a specific range of time and frequency. More details on the specific number and organization of regions are provided in Sect. 4.
- **Features Computation**. In this step, we compute the following five statistical features on each region defined in the previous step: (i) mean; (ii) standard deviation; (iii) variance; (iv) skewness; and, (v) kurtosis.

The output of this phase is a matrix of features that is passed either to the Training Module (PUF Manager) or to the Classification Module (verifier).

- **Training Module.** This module, installed on the PUF Manager, is responsible for using the features matrix produced by the *Features Extraction Module* to train a ML model. The aim of the model is to discriminate uniquely the devices and the responses of the device to different reference functions. The trained ML model is made available online on request to the verifier, to be used in the authentication stage to authenticate different devices. In this work, we use a one-class Support Vector Machine (SVM) algorithm with cubic kernel to train the ML model, so as to uniquely identify each device and reference function. Indeed, for each class considered, the SVM algorithm creates a standalone profile mapping the acquired emissions [33].
- **Classification Module.** This module, installed on the verifier, is responsible for testing the profile of the recorded magnetic emissions from the IoT device against the trained ML model made available by the PUF Manager. For each test sample, the one-class SVM provides an evaluation score, indicating the likelihood that the particular sample belongs to a specific class in the trained ML model [33]. The closest the score is to the value 0, the more likely the sample is consistent with the tested model.

3.4 Phases of *MAG-PUF*

MAG-PUF includes two main phases, namely, the *Enrolment Phase* and the *Authentication Phase*, detailed below.



(a) Sequence diagram of the Enrolment phase of *MAG-PUF*.

(b) Sequence diagram of the different steps of the Authentication phase of *MAG-PUF*.

Fig. 2. Sequence diagrams of *MAG-PUF*.

Enrolment Phase. Figure 2a shows the sequence diagram of the Enrolment Phase. Upon manufacture and before deployment, the *PUF Manager* chooses at random several *reference functions*, and submits them to the prover, requesting their execution. Note that a *reference function* can be either a single specific operation or a combination of several operations. Moreover, due to the specific application, each system administrator can freely choose the reference functions most suitable for *MAG-PUF*. For instance, the system administrator can choose the primitives (or combinations thereof) providing the most unique profile of unintentional magnetic emissions for the IoT device.

At the same time, using the *Emissions Extraction Module*, the *PUF Manager* acquires the unintentional magnetic emissions generated by the prover while executing the specified reference function(s). For each tested reference function, using the *Features Extraction Module*, the *PUF Manager* extracts some features of the recorded signal, builds an SVM model using the *Training Module*, and uploads the model to an online database.

Authentication Phase. The Authentication phase steps are detailed in Fig. 2b. Upon any authentication exchange, the verifier extracts at random one (or more) of the reference functions whose profiles are available from the PUF Manager, and instructs the prover to execute such function(s). At execution time, the verifier records the unintentional magnetic emissions emitted from the prover thanks to the *Emission Extraction Module* and analyzes them, thanks to the *Features Extraction Module*, to extract the relevant features. Then, using the *Classification Module*, the verifier checks if the model of the features just extracted and computed match the available profile. If the profile acquired at run-time matches the one downloaded from the PUF Manager, the prover is authenticated. Otherwise, authentication fails.

4 Experimental Performance Assessment

In this section, we provide the results of our experimental assessment, carried out to evaluate the performance of *MAG-PUF*. Specifically, Sect. 4.1 introduces the experimental testbed, in Sect. 4.2 we report the results of our analysis, in Sect. 4.3 we report some performance metrics for PUF robustness, and finally, Sect. 4.4 summarizes our investigation.

4.1 Experimental Setup

In our experimental campaign, we used the following equipment.

– **Arduino Uno Boards**. We tested the performance of *MAG-PUF* with a set of 25 identical Arduino UNO IoT boards [45]. Each board is equipped with an 8-bit microcontroller ATmega328P, featuring a 16 MHz ceramic resonator, 2 KB of internal SRAM, and a 32KB of Flash memory.

- **Aaronia PBS2 EMC Probe set**. To collect the unintentional magnetic emissions response when running different reference functions, we used the Aaronia PBS2 EMC Probe Kit [1]. This equipment enables simple measurements in the frequency range from DC (1 Hz) to 9 GHz, as well as the monitoring of magnetic emissions. We used the PBS-H3 25 mm magnetic (H3) field antenna as a probe. The antenna is covered with an insulating layer that provides a safe measurement environment for the Arduino's oscillators and mains lines. The UBBV2 40dB EMC RF pre-amplifier is connected to the probe, providing for a clear distinction between the relevant signal and the background noise. The probe is connected via a low-impedance cable to a spectrum analyzer, used to collect and store the magnetic emissions.
- **Rohde & Schwarz FSW8 Spectrum Analyzer**. We used the Rohde & Schwarz FSW8 Spectrum Analyzer to record the unintentional magnetic emissions captured by the probe over a large frequency span, up to 80 MHz. This equipment converts raw I-Q samples into spectral power density measurements. Specifically, it performs a Fast Fourier Transform (FFT) on the collected data and, for each time frame, it generates a tuple containing the timestamp (in ms), the frequency (in Hz), and the power level (in dBm).
- **Matlab R2021a**. Matlab R2021a has been used to extract features from the collected magnetic emissions data of different reference functions run by the Arduino IoT devices. Matlab was also used to train and test the ML model for the classifications of samples, using the one-class SVM model with a cubic kernel as the classification algorithm.

All the experiments described below have been conducted in regular laboratory conditions, without any effort to reduce the environmental noise. Our measurement setup is shown in Fig. 3.

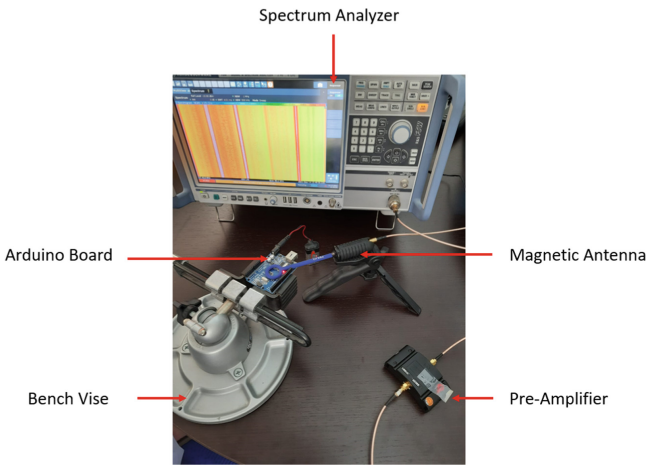


Fig. 3. Measurements setup

We placed the Arduino board on a Bench Vise, to hold it in a fixed position and allow for uniform recording conditions. We also placed the magnetic antenna directly above the IoT boards, to clearly capture the magnetic emission from the micro-controller and surrounding chips. The position of the magnetic antenna can be precisely controlled by a mechanical arm to ensure consistent positioning on the Arduino device in each sample collection. Alternatively, a special opening in the cover case of Arduino device can be made to exactly fit the magnetic antenna, ensuring precise placement with every measurement. Finally, we saved the collected emissions from each reference function run on the Arduino on the Spectrum analyzer.

4.2 Experimental Results

In the following, we provide several experimental results.

Spectral Power Density of Sample Reference Functions. We first evaluated the profile of unintended magnetic emissions generated by an Arduino IoT device when running different reference functions. To this aim, we defined the following operations: (A1) empty loop; (A2) first encrypt, later decrypt a 128 bit long message, using AES128, Block Cipher Mode (CBC); (A3) comparison of the similarity between two 11-bytes long strings; and, (A4) reading of input data from a DHT11 temperature and humidity sensor. We use the above-listed reference functions as examples to test our proposed *MAG-PUF* solution, as they are supported by almost any IoT device. Note that the usage of AES does not contradict our initial hypothesis on the constraints affecting IoT devices. Indeed, even if IoT devices could support symmetric encryption algorithms, they often cannot feature effective re-keying algorithms, being those often based on public-key cryptography. We also recall that each system administrator can choose the reference functions she finds most suitable for *MAG-PUF*, e.g., choosing the ones that provide the most unique profile of unintentional magnetic emissions for the device.

Figure 4 shows the spectral power density of the unintentional magnetic emissions of the full 80 MHz bandwidth acquired by the spectrum analyzer, with reference to the functions defined above, separated by dashed black lines. Each function lasts for around 120 ms. Because of the normalization phase executed during the *Features Extraction module*, all the RSS of samples of unintentional magnetic emissions recorded in dBm are normalized to a value between 0 and 1. Specifically, the blue color corresponds to values in the range [0–0.25], the cyan maps values in the range [0.25–0.5], the yellow indicates values in the range [0.5–0.75], while the red color is related to values in the range [0.75–1].

First, we can notice the clear color differences in the spectral power density between (A1) and (A3) compared with (A2) and (A4). Indeed, (A2) and (A4) are computationally-intensive operations, which require more processing power than (A1) and (A3). Furthermore, we can also see the similarity between the unintentional magnetic emissions of (A1) and (A3). Indeed, the string comparison operation (A3) is lightweight, it does not involve any complex mathematical

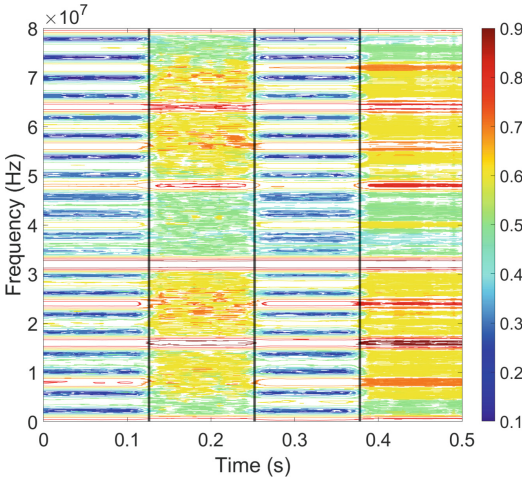


Fig. 4. Unintentional magnetic emissions recorded for around 120 ms of each of the four reference functions, using 80 MHz bandwidth, separated by black lines. (Color figure online)

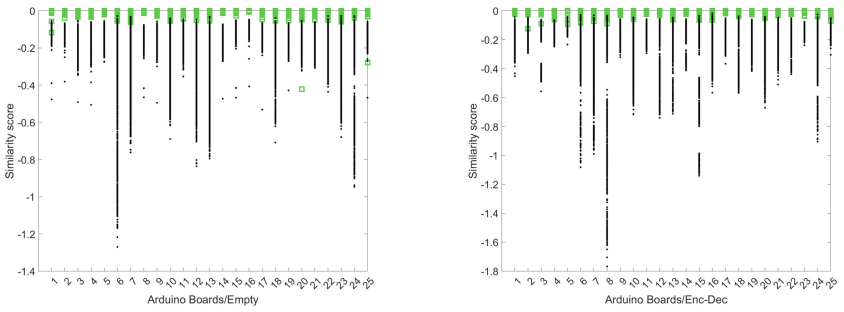
operations, and it does not consume much more processing power than (A1), leading to similar spectral power profiles. We recall that the system administrator can select the best reference functions for its objective, i.e., the ones with distinct unintentional magnetic emissions, excluding others achieving worst performances in the field, so as to guaranteeing reliable IoT devices authentication. Overall, the results above demonstrate the fulfilment of the *Constructibility* requirement introduced in Sect. 2.3, as the PUF can be constructed by invoking the specific function, as well as the PUF *Evaluability*, being x the function run by the prover and y the unique profile of the emissions generated for each PUF.

Classification Results. For the verifier to authenticate the prover, we utilize the MATLAB provided one-class cubic SVM ML model. We consider the functions above described, each run separately inside a *For* loop on each of the 25 IoT boards. We collected the related magnetic emanations for around $6,000$ slot-frames, each lasting 12 ms long. We divided each trace into 10 frames segments, getting 600 samples for each trace of the magnetic emanations recorded on a given IoT board when running a specific function. With the described procedure, the duration of a single instance of a function is 8 ms, i.e., each segment (120 ms) comprises the magnetic emanations of around 15 iterations of a given function. We collected each trace twice across four different days, to ensure robustness against temporary phenomena in the surrounding environment. This procedure resulted in $600 \cdot 2 = 1,200$ samples of each function running on each individual IoT board. We divided those $1,200$ samples into 80% (960 samples) for training of the ML model, and the remaining 20% (240 samples) for testing the trained model. Overall, we have 25 IoT boards, with 960 samples for each

reference function, returning 24,000 samples of each reference function for training, and 25 boards with 240 samples of each reference function, returning 6,000 samples of each reference function running on the 25 IoT boards for testing.

As a result of many experiments and tests, we considered a 20 MHz acquisition bandwidth and a fixed observation window of 10 frames (120 ms) for each of the collected traces of magnetic emissions, to allow a fair cross-comparison between different traces. Each time window is further divided into a number of time and frequency regions. Then, we computed the following five statistical features over each of them: mean, standard deviation, variance, skewness, and kurtosis. Overall, we considered 95 features, computed as follows. First, we computed the five (5) statistical features over the whole observation window of 10 frames (120 ms), generating 5 features. Then, we further divided the observation window of 120 ms into two time regions, each 60 ms long, and we computed the same 5 statistical features for each of them, resulting in 10 additional features. Then, we further divided each of the time regions generated in the previous step into eight (8) frequency regions, each with a bandwidth of 2.5 MHz. For each of the $2 \cdot 8$ frequency regions, we computed the same aforementioned five statistical features, resulting in $2 \cdot 8 \cdot 5 = 80$ features. By summing the three stages, we have a total of $5 + 10 + 80 = 95$ features.

For each IoT board, we report the data coming from the authentic IoT device as green squares (240 samples per class), while the black dots (5,760 samples) represent the non-authentic ones. In the vast majority of experiments, the authentic IoT devices reported values very close to 0, while the other IoT devices executing even the same function reported lower scores. Given that the model of each IoT device is trained and validated on its own, we selected a threshold value for each one, and we decided to accept it as authentic if the evaluation score is higher than the selected threshold.

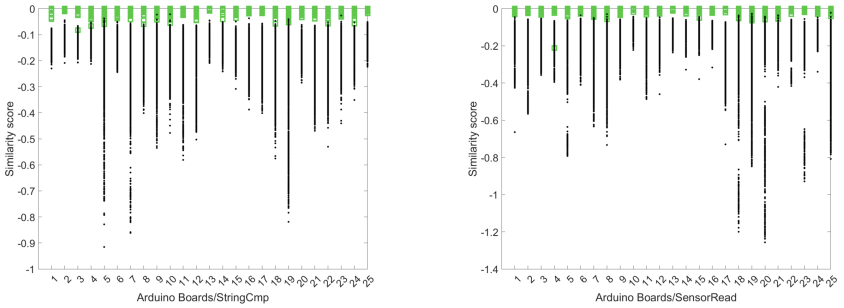


(a) Classification results of (A1) on 25 IoT devices, using 20 MHz bandwidth.

(b) Classification results of (A2) on 25 IoT devices, using 20 MHz bandwidth.

Fig. 5. Classification results for reference functions (A1) and (A2).

Figures 5a, 5b, 6a, and 6b show the similarity scores generated by the cubic SVM model, produced by the considered IoT boards' classes, each considering



(a) Classification results of (A3) on 25 IoT devices, using 20 MHz bandwidth.

(b) Classification results of (A4) on 25 IoT devices, using 20 MHz bandwidth.

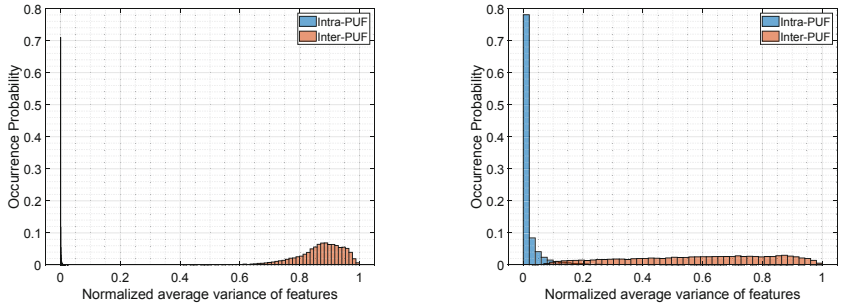
Fig. 6. Classification results for reference functions (A3) and (A4).

specific reference functions, using 20 MHz out of the total 80 MHz acquired bandwidth, over the 95 features previously-described. The average accuracy of each function across the IoT boards is 99.3%, 99.4%, 99.7%, and 99.6%, respectively. Such remarkable performances definitely prove also the *uniqueness* and *reproducibility* of *MAG-PUF* (see Sect. 2.3).

4.3 PUF Robustness Evaluation

In this section, we discuss the feasibility of using magnetic emissions as PUFs, through the *Intra-PUF Distance* (as a measure for the PUF *Reliability*) and *Inter-PUF Distance* (as a measure of the PUF *Uniqueness*).

We recall, from Sect. 2.3, that the *Intra-PUF Distance* provides insights into the reliability of a PUF, while the *Inter-PUF Distance* represents the uniqueness of the PUF. We cannot use the standard Intra-PUF and Inter-PUF Hamming distances to evaluate *MAG-PUF* since, differently from traditional PUFs discussed in Sect. 5, *MAG-PUF* does not produce a digital response. Conversely, *MAG-PUF* utilizes the differences of magnetic profiles produced as a response when similar reference functions are run on IoT boards. Indeed, from the *MAG-PUF* classification accuracy detailed in Sect. 4.2, we can confirm the reliability and uniqueness of our solution. In addition, Fig. 7a reports the Intra-PUF and Inter-PUF distances as the normalized average of the variance of the most prominent 20 statistical features used for ML classification. We computed the *Inter-PUF Distance* as the average variance of 600 groups, each group consisting of 25 magnetic samples taken from specific IoT device when executing a specific function, e.g., (A1) in Fig. 7a (other functions produced similar results, and are omitted for the sake of space). Each sample contains the top 20 features extracted at 20 MHz bandwidth. The *Intra-PUF Distance*, instead, is computed as the average variance of the features of 600 samples of each IoT device. Note that the most prominent normalized average variance for the Intra-PUF Distance (same device) is in the range [0–0.0005], while it is in the range [0.8–1] for



(a) Average variance of the most prominent 20 features extracted at 20 MHz bandwidth from each IoT board.

(b) Average variance of the 95 features extracted at 20 MHz bandwidth from each IoT board.

Fig. 7. Average variance of the features extracted from the 25 IoT boards.

the Inter-PUF Distance (different devices). The ideal values of the *Inter-PUF Distance* and *Intra-PUF Distance* discussed in the literature are ≈ 0.5 and 0, respectively [26]. In our case, the geometric mean of the normalized average variance of the 95 features used in *MAG-PUF*, reported in Fig. 7b, is approx. 0.51 for the *Inter-PUF Distance* and 0.02 for the *Intra-PUF Distance*, almost coincidental with the optimal values. Such results prove the reliability and uniqueness of *MAG-PUF*, and the suitability of the usage of magnetic emissions as PUFs.

4.4 Discussion and Limitations

Impact of the Environmental Noise. As mentioned in Sect. 4.1, we used a near field magnetic antenna to collect the emissions of the IoT devices. Such a setup allows for transparently mitigating the effect of surrounding environmental noises, as the antenna only captures a small near field around its location, i.e., on top of the electronic chips of the device. In addition, since any PUFs are susceptible to noise, the authentication can be done using a set threshold of multiple CRP to check against the CRP database. This threshold of CRP can be proportional to the amount of noise in the environment and to the total number of PUF devices that need to be distinguished [20].

PUF Replay and Reuse Attacks. The main attack applicable on PUFs is the replay and reuse attack, where the adversary has a temporary access to the PUF during the authentication exchange. This allows the opportunity for modeling the responses and launching a replay attack. Conversely to the RF-PUF proposed in [8], our solution enjoys the possible usage of a potentially unlimited number of reference functions. As such, *MAG-PUF* can abide to a one-time use protocol [30], so as to prevent PUF reuse and modeling attacks. In one-time use protocols, each nonce (in our case, reference function) is used only once, thus not being re-usable in case of replay and reuse.

Scaling up CRPs Pairs. Using *MAG-PUF*, several methods can be adopted to scale up CRPs pairs. One is to use different reference functions. As depicted in Fig. 4, each reference function has a unique profile of unintentional magnetic emissions, depending on the utilization of the micro-controller resources. To accommodate a large number of IoT devices, different reference functions can be used for specific sets of provers. Moreover, different reference function combinations and different acquisition bandwidths can also be used to scale up CRP pairs.

ML Modeling Attacks. *MAG-PUF* can also be the target of ML-based attacks, aiming at modeling the magnetic emission responses to reference functions through repeated eavesdropping of the exchanged authentication CRPs. On the one hand, *MAG-PUF* utilizes supervised ML to identify the magnetic emissions radiated when executing specific reference functions. On the other hand, as discussed in [8], the attacker would have to resort to unsupervised ML approaches to classify the eavesdropped CRPs streams. Thus, the modeling time is proportional to the number of CRPs possessed by attacker, and the accuracy of the model depends on the ratio of the CRPs possessed to the total length of the CRP database [11]. As discussed above, *MAG-PUF* can be scaled to use theoretically unlimited number of reference functions, and thus, CRPs pairs, making the task of such attacker harder.

Table 1. Qualitative comparison of *MAG-PUF* against competing solutions.

Ref.	Type	Strong PUF	No RF interface	Near-field emissions	Hardware-agnostic
[8]	RF	✓	✗	✗	✓
[15]	RF	✓	✗	✓	✗
[10]	RF	✓	✗	✓	✗
[31,44]	Delay	✓	✓	N/A	✗
[4,27,47]	Delay	✗	✓	N/A	✗
[2,6]	Memory	✓	✓	N/A	✗
[23]	Memory	✗	✓	N/A	✗
[9,13,14,17]	Memory	✗	✓	N/A	✗
[25]	Memory	✗	✓	N/A	✗
[43]	Memory	✗	✓	N/A	✗
MAG-PUF	Magnetic	✓	✓	✓	✓

5 Related Work and Comparison

MAG-PUF enforces authentication using unintentional magnetic emissions radiated by IoT devices when executing specific functions, such as PUFs. A preliminary discussion of this idea appears in [18]. Thus, both EM-based *code fingerprinting* and PUF techniques are closely related to our work.

EM-based Code Fingerprinting. Code fingerprinting techniques leveraging Electro-Magnetic (EM) emissions have been used for several purposes. For instance, Sehatbakhsh *et al.* [38] introduced an EM physical side-channel vulnerability caused by the regular use of power management units in computers. Using such a side-channel, an attacker can create a covert channel to extract sensitive information. Similarly, Sangodoyin *et al.* [32] leveraged EM signals leaked from IoT devices to infer on programs activities and extract information. Sehatbakhsh *et al.* [36] presented EMMA, i.e., an attestation method based on EM emanations emitted from the prover when executing specific code. Both the above schemes are used to attest the functions execute by the device, but not to authenticate it. Another contribution is IDEA [21,22], i.e., a framework exploiting EM emanations to detect anomalous activities on embedded devices and Cyber-Physical Systems (CPS). Additional contributions for EM-based detection of Malware and deviations in program execution are presented in [5,16,29,35,37]. Moreover, Ibrahim *et al.* [19] used unintentional magnetic emissions to fingerprint USB flash drives. Their approach fingerprints the boot of the USB device, thus being not applicable for run-time authentication. Overall, the cited works prove the feasibility of using EM emanations to fingerprint specific devices' functions, but were never applied for run-time authentication.

Physical Unclonable Functions. From their introduction in [12], several PUFs have been proposed.

Delay-based PUFs use delays in the ICs of the devices for authentication. To name a few, Suh et al. [44] used them for authentication and secret key generation, while the authors in [31,48] designed multiplexer-based arbiter PUFs.

Radio-frequency (RF)-based PUFs exploit non-idealities in the transmitted RF signals for authentication. For instance, Deejan et al. [10] introduced RF-based Certificates of Authenticity (COA) to identify counterfeits, Chatterjee et al. [8] used deep neural networks to identify wireless transmitters, while Guajardo et al. [15] leveraged the peaks in the frequency response of IC to identify them.

Memory-based PUFs authenticate devices based on unique randomness of memory elements. To name a few, the authors in [2,6] used the randomness in the Resistive Random Access Memory (ReRAM), while the authors in [9,13,17], and [14] focused on the power-up of the static random access memory (SRAM). Other elements used are flip-flops [25] and latches [43].

Table 1 summarizes the PUF contributions above discussed, along relevant features. A novel element characterizing *MAG-PUF* is the independence from specific hardware. In addition, the magnetic emanations used by *MAG-PUF* can be captured mainly from the near-field of the prover, requiring the attacker to be in close proximity. Conversely, RF-based PUFs emissions can be eavesdropped from long distances, widening the attack scenario. *MAG-PUF* provides also a Strong PUF, easily allowing for the extraction of a large number of challenge-response pairs, and it does not require the presence of any RF interface in the device, as in the case of RF PUFs. Finally, *MAG-PUF* can utilize a theoretically

unlimited number of reference functions; conversely, RF-PUFs use wireless messages, leveraging mostly identical digital data-streams.

6 Conclusions

In this paper, we proposed *MAG-PUF*, a novel and lightweight physical-layer authentication solution for resource-constrained IoT devices. *MAG-PUF* authenticates IoT devices using the uniqueness of the unintentional magnetic emissions radiated by the devices when executing specific functions. Our conceptual framework is supported by an extensive experimental campaign. Using 25 Arduino IoT boards and a set of exemplary reference functions, we revealed an outstanding classification accuracy (over 99%), high flexibility, robustness, and very limited overhead. At the same time, our investigation shows the robustness of using magnetic emissions for PUFs, with relevant metrics very close to the ideal values.

Overall, *MAG-PUF* emerges as an ideal solution to authenticate constrained IoT devices, especially where field devices cannot afford complex cryptography operations. Future work will consider the extraction of emissions on the IoT devices, with the integration of very-low bandwidth embedded magnetic sensors.

Acknowledgements. This publication was partially supported by award GSRA6-1-0528-19046, from the QNRF-Qatar National Research Fund, a member of Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF. This publication was also partially supported by the INTERSECT project, Grant No. NWA.1162.18.301, funded by Netherlands Organization for Scientific Research (NWO) and the NATO Science for Peace and Security Programme - MYP G5828 project "SeaSec: DronNets for Maritime Border and Port Security".

References

1. Aaronia: PBS2 EMC Probe (2021). https://tinyurl.com/2syhszbw, Accessed 31 July 2022
2. Afghah, F., Cambou, B., Abedini, M., Zeadally, S.: A reram physically unclonable function (reram puf)-based approach to enhance authentication security in software defined wireless networks. Int. J. Wirel. Inf. Netw. **25**(2), 117–129 (2018)
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015)
4. Bossuet, L., Ngo, X.T., Cherif, Z., Fischer, V.: A puf based on a transient effect ring oscillator and insensitive to locking phenomenon. IEEE Trans. Emerg. Topics Comput. **2**(1), 30–36 (2013)
5. Callan, R., Behrang, F., Zajic, A., Prvulovic, M., Orso, A.: Zero-overhead profiling via em emanations. In: Proceedings of the 25th International Symposium on Software Testing and Analysis, pp. 401–412 (2016)
6. Cambou, B., Orlowski, M.: Puf designed with resistive ram and ternary states. In: Proceedings of the 11th Annual Cyber and Information Security Research Conference, pp. 1–8 (2016)

7. Camurati, G. et al.: Screaming channels: when electromagnetic side channels meet radio transceivers. In: ACM CCS, pp. 163–177 (2018)
8. Chatterjee, B., Das, D., Maity, S., Sen, S.: Rf-puf: enhancing IoT security through authentication of wireless nodes using in-situ machine learning. IEEE Internet Things J. **6**(1), 388–398 (2018)
9. Claes, M., van der Leest, V., Braeken, A.: Comparison of SRAM and FF PUF in 65 nm technology. In: Laud, P. (ed.) NordSec 2011. LNCS, vol. 7161, pp. 47–64. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29615-4_5
10. DeJean, G., Kirovski, D.: RF-DNA: radio-frequency certificates of authenticity. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 346–363. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_24
11. Delvaux, J., Verbauwhede, I.: Side channel modeling attacks on 65 nm arbiter PUFs exploiting CMOS device noise. In: 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 137–142. IEEE (2013)
12. Gassend, B., Clarke, D., Van Dijk, M., Devadas, S.: Silicon physical random functions. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 148–160 (2002)
13. Guajardo, J., Kumar, S.S., Schrijen, G.-J., Tuyls, P.: FPGA intrinsic PUFs and their use for IP protection. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 63–80. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_5
14. Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: Physical unclonable functions and public-key crypto for fpga ip protection. In: 2007 International Conference on Field Programmable Logic and Applications, pp. 189–195. IEEE (2007)
15. Guajardo, J.: Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. Inf. Syst. Front. **11**(1), 19–41 (2009)
16. Han, Y., Etigowni, S., Liu, H., Zonouz, S., Petropulu, A.: Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1095–1108 (2017)
17. Holcomb, D.E., Burleson, W.P., Fu, K.: Power-up sram state as an identifying fingerprint and source of true random numbers. IEEE Trans. Comput. **58**(9), 1198–1210 (2008)
18. Ibrahim, O.A., Sciancalepore, S., Di Pietro, R.: Mag-puf - authenticating iot devices via magnetic physical unclonable functions. In: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2022, pp. 290–291. ACM, New York (2022)
19. Ibrahim, O.A., Sciancalepore, S., Oligeri, G., Pietro, R.D.: Magneto: fingerprinting usb flash drives via unintentional magnetic emissions. ACM Trans. Embedded Comput. Syst. (TECS) **20**(1), 1–26 (2020)
20. Islam, M.N., Kundu, S.: Enabling ic traceability via blockchain pegged to embedded puf. ACM Trans. Des. Autom. Electron. Syst. (TODAES) **24**(3), 1–23 (2019)
21. Khan, H.A., Sehatbakhsh, N., Nguyen, L.N., Prvulovic, M., Zajić, A.: Malware detection in embedded systems using neural network model for electromagnetic side-channel signals. J. Hardware Syst. Secur. **3**(4), 305–318 (2019)
22. Khan, H.A., et al.: Idea: intrusion detection through electromagnetic-signal analysis for critical embedded and cyber-physical systems. IEEE Trans. Depend. Secure Comput. (2019)
23. Kumar, S.S., Guajardo, J., Maes, R., Schrijen, G.J., Tuyls, P.: The butterfly puf protecting ip on every fpga. In: 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 67–70. IEEE (2008)

24. Maes, R.: Physically Unclonable Functions: Constructions, Properties and Applications. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41395-7
25. Maes, R., Tuyls, P., Verbauwhede, I.: Intrinsic pufs from flip-flops on reconfigurable devices. In: 3rd Benelux Workshop on Information and System Security (WISSec 2008), vol. 17, p. 2008 (2008)
26. Maiti, A., Casarona, J., McHale, L., Schaumont, P.: A large scale characterization of ro-puf. In: 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 94–99. IEEE (2010)
27. Maiti, A., Schaumont, P.: Improved ring oscillator puf: an fpga-friendly secure primitive. J. Cryptol. **24**(2), 375–397 (2011)
28. McGrath, T., et al.: A PUF taxonomy. Appl. Phys. Rev. **6**(1), 011303 (2019)
29. Nazari, A., Sehatbakhsh, N., Alam, M., Zajic, A., Prvulovic, M.: Eddie: em-based detection of deviations in program execution. In: Proceedings of the 44th Annual International Symposium on Computer Architecture, pp. 333–346 (2017)
30. Ostrovsky, R., Scafuro, A., Visconti, I., Wadia, A.: Universally composable secure computation with (malicious) physically uncloneable functions. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 702–718. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_41
31. Sahoo, D.P., Mukhopadhyay, D., Chakraborty, R.S., Nguyen, P.H.: A multiplexer-based arbiter puf composition with enhanced reliability and security. IEEE Trans. Comput. **67**(3), 403–417 (2017)
32. Sangodoyin, S., et al.: Remote monitoring and propagation modeling of em side-channel signals for iot device security. In: 2020 14th European Conference on Antennas and Propagation (EuCAP), pp. 1–5. IEEE (2020)
33. Schölkopf, B., Smola, A.J., Bach, F., et al.: Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond. MIT press, Cambridge (2002)
34. Sciancalepore, S., Oligeri, G., Piro, G., Boggia, G., Di Pietro, R.: EXCHANge: securing IoT via channel anonymity. Comput. Commun. **134**, 14–29 (2019)
35. Sehatbakhsh, N., Alam, M., Nazari, A., Zajic, A., Prvulovic, M.: Syndrome: spectral analysis for anomaly detection on medical iot and embedded devices. In: 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 1–8. IEEE (2018)
36. Sehatbakhsh, N., Nazari, A., Khan, H., Zajic, A., Prvulovic, M.: Emma: Hardware/software attestation framework for embedded systems using electromagnetic signals. In: Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture, pp. 983–995 (2019)
37. Sehatbakhsh, N., Nazari, A., Zajic, A., Prvulovic, M.: Spectral profiling: observer-effect-free profiling by monitoring em emanations. In: 2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), pp. 1–11. IEEE (2016)
38. Sehatbakhsh, N., Yilmaz, B.B., Zajic, A., Prvulovic, M.: A new side-channel vulnerability on modern computers by exploiting electromagnetic emanations from the power management unit. In: 2020 IEEE International Symposium on High Performance Computer Architecture (HPCA), pp. 123–138. IEEE (2020)
39. Semiconductor Eng.: IoT Device Security Makes Slow Progress (2019). https://semiengineering.com/iot-device-security-makes-slow-progress/, Accessed 31 July 2022
40. Shamsoshoara, A., Korenda, A., Afghah, F., Zeadally, S.: A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Comput. Netw. **183**, 107593 (2020)

41. Siow, E., et al.: Analytics for the Internet of Things: a survey. ACM Comput. Surv. (CSUR) **51**(4), 1–36 (2018)
42. Statista: Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 (2020). https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/, Accessed 31 July 2022
43. Su, Y., Holleman, J., Otis, B.P.: A digital 1.6 pj/bit chip identification circuit using process variations. IEEE J. Solid-State Circ. **43**(1), 69–77 (2008)
44. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: 2007 44th ACM/IEEE Design Automation Conference, pp. 9–14. IEEE (2007)
45. Treedix: Arduino UNO (2021). https://tinyurl.com/TreedixArduinoUNO, Accessed 31 July 2022
46. Tuyls, P., Škoric, B., Kevenaar, T.: Security With Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer, Heidelberg (2007). https://doi.org/10.1007/978-1-84628-984-2
47. Yin, C.E., Qu, G.: Temperature-aware cooperative ring oscillator puf. In: 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 36–42. IEEE (2009)
48. Zalivaka, S.S., Ivaniuk, A.A., Chang, C.H.: Reliable and modeling attack resistant authentication of arbiter puf in fpga implementation with trinary quadruple response. IEEE Trans. Inf. Forensics Secur. **14**(4), 1109–1123 (2018)