A PUF Sensor: Securing Physical Measurements

Hua Ma†, Yansong Gao†, Omid Kavehei‡, and Damith C. Ranasinghe†
†Auto-ID Labs, School of Computer Science, The University of Adelaide, SA 5005, Australia
{mary.ma, yansong.gao, damith.ranasinghe}@adelaide.edu.au
‡School of Electrical and Computer Engineering, Royal Melbourne Institute of Technology, VIC 3001, Australia
omid.kavehei@rmit.edu.au

***Abstract*—Sensors are important components in the Internet of Things (IoT) that encompass a wide spectrum of applications from healthcare to monitoring critical infrastructure. Securely gathering sensor measurements by adopting traditional cryptographic mechanisms is fraught with vulnerabilities emanating from the inability to safeguard secrets on edge devices, often in adversarial environments, where appropriate hardware protection logic and power consumption overheads are counterproductive to the desire to keep the devices low cost and long lasting. This paper continues recent efforts into investigating an alternative secure sensing approach with the potential to provide a solution for resource-restricted IoT devices. In particular, we investigate the possibility to exploit unreliability of a physical unclonable function (PUF) resulting from its sensitivity to variations in supply voltage conditions to guarantee the veracity of physical measurements from potentially any transducer capable of converting a physical phenomenon to a voltage signal. Therefore we present an approach that has the potential to realize a *universal* PUF sensor where the PUF itself acts as a sensor or is integrated with a sensor. Thus, for a PUF sensor, cryptographic processes and sensing are inseparable. Further, we rely on a dominant external condition—voltage—responsible for unreliability to secure sensing. We validate the feasibility of the proposed universal PUF sensor approach based on experimental data extracted from RO-PUFs (Ring Oscillator PUFs).**

***Index Terms*—PUF sensor, secure sensing, hardware security, physical unclonable function.**

I. Introduction

Smart devices are increasingly integrated and introduced into every domain of our lives. Networking of smart devices, commonly known as the Internet of Things (IoT), support a broad ranges of applications in both commercial and industrial sectors [1]. Often, tiny sensor nodes are tentacles of such a network that sense the environment, collect and communicate sensitive and critical information [2], [3]. Therefore, the ablility to securely send such infomation where the receiver has the ability to determine the veracity or trust is paramount. However, IoT devices are often resource constrained in terms of cost, computational capacity and power. Therefore, a traditional cryptographic solution that relies on a separate crypto module are naturally less appealing to those small(er) low-end devices, where there is usually no dedicated room for securely implementing crptographic primitives and securing private keys within non-volatile memory (NVM)—as keys can be extracted [4] by a motivated attacker.

The physical unclonable function (PUF) is a lightweight hardware security primitive. They are increasingly employed to serve as hardware trust anchors of resource-constrained devices [5]–[8]. A PUF extracts secrets on demand from the imperfections or uncertainties of a hardware device introduced during fabrication. A PUF cannot be physically cloned and very hard, if not impossible, to be physically attacked since, unlike NVMs, secrets are not stored but rather extracted. The PUF maps an input (*challenge*) to an output (*response*) through a complex physical function that is mathematically analogous, in general, to an instance-specific hash function. Therefore, responses differ significantly from different PUF instances given the same queried challenge, even if these PUF instances have identical design and are fabricated by the same manufacturer.

A PUF is expected to regenerate the same response when queried by the same challenge. However, in practice, reliable response regeneration is influenced by environment factors. In typical PUF-based applications, for instance, cryptographic key generation requiring highly stable responses [9], it is imperative to improve PUF reliability and correct potential bit errors prior to deriving a key. In PUF-based authentication applications [6], [7], [10], it is preferable to maximize reliability to reduce the number of response bits needed to uniquely identify a PUF instance and increase the complexity of modeling attacks by an adversary [11]–[13].

In contrast, we exploit this unavoidable unreliability to provide a high degree of assurance to the sensed data where the PUF itself is a sensor. Specifically, we exploit those challenges that yield unreliable response bits that change from one state ‘0’/‘1’ to its opposing state ‘1’/‘0’ in response to an environmental parameter change. Notably, such a response bit can be reproduced consistently for a given environmental condition. The relationship between unreliable response bits and the environmental parameters allows a potential new paradigm for securing sensing where the PUF itself is used as a sensor or is seamlessly integrated with a sensor.

The concept of employing a PUF to sense a particular physical quantity (PQ)—an environmental parameter—was presented by Rosenfeld *et al.* [14]. Here, the PUF takes not only the challenge but also a PQ—light is considered in [14]—as its inputs. Hence, the response is mapped from two inputs instead of one. The motivation is to merge sensing with cryptography. In [15], Rajendran *et al.* merge pressure sensing with a PUF. Ruhrmair *et al.* [16], [17] selected temperature as a PQ to experimentally demonstrate their new security concept, *virtual proof of reality*, that assures the proof of a physical statement over an untrusted digital communication channel

978-1-5090-4338-5/17/$31.00 ©2017 IEEE

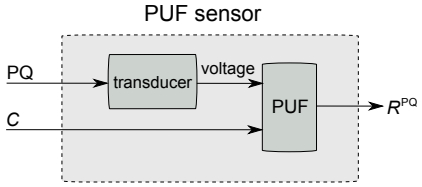

Figure 1. A universal PUF sensor architecture based on exploiting dominant response sensitivity to voltage. This approach allows the possibility to sense other PQs by converting them into a voltage by an on-chip transducer.

between two parties (a "prover" and a "verifier") without cryptographic algorithms.

Instead of only sensing a specific PQ, eg., temperature [16] or light [14], sensing electrical signals—eg., voltage—is more attractive, because the chosen electrical parameter is versatile. Various types of PQs such as temperature, humidity, sound energy, can eventually be converted into electrical signals using a transducer that can be used to influence the reliability of a PUF. The proposed PUF sensor architecture is illustrated in Fig. 1. In this approach, other PQs are able to be securely sensed indirectly through the corresponding electrical signals. Hence an approach to securely sense voltage could serve as a *universal* PUF sensor. In addition, such a PUF sensor exploits the most dominant external condition—supply voltage—responsible for response unreliability of popular circuit based PUF designs such as Arbiter PUFs or Ring Oscillator PUFs that can be easily realized in standard CMOS (Complementary Metal-Oxide Semiconductor) technology.

Our contributions in this paper are:

1) We propose a potential *universal* PUF sensor architecture by exploiting the relationship between unreliable response bits and a versatile external parameter—supply voltage.
2) We validate the feasibility of our proposed secure sensing methodology using a ring oscillator PUF (ROPUF) to correctly discover voltage values. Other PQs can be converted into a voltage using corresponding transducers to influence the unreliable response behaviour and consequently be recovered by the same sensing methodology.
3) We observe that only the unreliable responses contribute to secure sensing. Thus, we present a method to expedite the selection of unreliable response bits that are highly sensitive to voltage variations and hence employ those selected response bits to greatly ease the recovery of a PQ by verifier or a server.

The rest of the paper is organized as follows. Related work is introduced in Section II. In Section III, we describe how the relationship between supply voltage and responses to a given set of challenges, often discarded from typical security related applications, can be exploited to construct a PUF sensor by using an ROPUF as a case study. Then experimental validation of the proposed secure sensing approach is presented in Section IV along with an approach to increase the sensing capability through the pre-selection of unreliable challenges. In Section V we conclude this article and discuss several challenges that must be addressed in the future.

II. Related Work

In general, a PUF sensor makes use of auxiliary physical effects to alter challenge-response mapping relationships in a conventional PUF construction. Rosenfeld *et al.* [14] first conceived the use of a PUF as a sensor to overcome the need for a separate crypto module that relies on conventional cryptographic algorithms to encrypt sensed values. They validated the concept by sensing light using simulated data. In [15], Rajendran *et al.* validated a micro-electro-mechanical relay based PUF sensor to sense pressure using simulation results. These two works demonstrated that PUF responses can be treated not only as a function of the challenges as in traditional PUF constructions but also a function of a second input—a specific PQ—and thus providing the capability for secure sensing. Ruhrmair *et al.* [16], [17] also examined the PUF sensor concepts and experimentally demonstrated the idea of *virtual proof of reality* (VP)—a security concept complementary to physical zero-knowledge protocols [18]—that assures the proof of a physical statement over an untrusted digital communication channel from the prover to the verifier without relying on cryptographic algorithms. In this approach, a prover *first* claims a physical statement and then proves it to the verifier. The concept was demonstrated using experimental results based on sensing temperature. All the above works demonstrate that PUF sensors can actually sense and hide from an adversary specific physical measurements.

In contrast to a PUF sensor that is solely applicable to sense a specific PQ, such as pressure, light or temperature, we take advantage of unwanted and inherent PUF response unreliability in conventional PUF applications to discover the operating voltage of a PUF when it influences the response reliability to realize a potential universal PUF sensor framework. From a different perspective, we take advantage of voltage as an input to remap challenge response pairs. Technically, it is similar to the concept of a reconfigurable PUF where external effects are used to reconfigure challenge-response behaviour [19]–[21]. In [20], Sharif *et al.* used multiple supply voltages to alter the challenge-response pair behavior by reconfiguring each inverter in a ring oscillator (RO), individually, to increase the number of CRPs of an ROPUF. In contrast, we propose exploiting the altered challenge-response behavior induced by a voltage change to recover the altered voltage for secure sensing of a range of physical quantities.

III. Secure Sensing Concept

Response unreliability is a natural PUF feature. The unreliability of a PUF is characterized by the fact that two regenerated response bits given the same randomly chosen challenge query to the same PUF instance can be different, [22]. Notably, PUF response unreliability is mainly induced by environmental parameter shifts, for example, supply voltage or temperature. In other words, responses differ when they are re-evaluated across a range of operating conditions, but a specific response bit is reproducible given the same operating condition. More specifically, the regeneration of a response bit r across a wide range of PQ may be inconsistent, but it is still reproducible

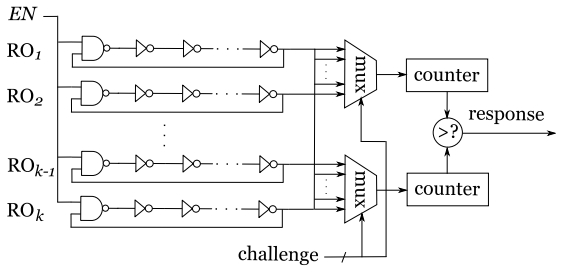

Figure 2. Typical structure of a ring oscillator PUF (ROPUF).

or retrievable under a certain fixed value of this PQ. In this paper, we detail the rationale using an ROPUF.

As shown in Fig. 2, a typical ROPUF structure consists of k ROs, two k-to-1 multiplexers that select a pair of ROs, RO_i and RO_j, two counters and a comparator [7]. All ROs are designed identically. Ideally, the frequency of each oscillator should be equal. However, because the oscillating frequency is a function of physical device parameters subject to process variations, the oscillation frequencies of different oscillators are not identical. Therefore, the oscillation frequencies of each pair are compared by counting the frequency using the digital counters. If $f_i < f_j$, where f_i and f_j are the oscillating frequencies of RO_i and RO_j, respectively, the digital comparator output will be '0', otherwise '1'. The pairing of oscillators is controlled using two digital multiplexers; each uses a subset of the input challenge bits to select an RO.

Moreover, the frequency of an RO has an almost linear relationship with its supply voltage. The coefficient, determining the relationship, however, varies from one RO to the other. In detail, as depicted in Fig. 3, the coefficient of RO_1 is higher than the coefficient of RO_3 because RO_1 oscillates faster than the RO_3 as the supply voltage increases. Here, the challenge bit c_3 selects an RO pair—RO_1 and RO_3—in order to produce a response bit r_3 by comparing f_1 and f_3. When a response bit is regenerated under a voltage located at the crosspoint of f_1 and f_3—between V_2 and V_3 at p_2, the response bit r_3

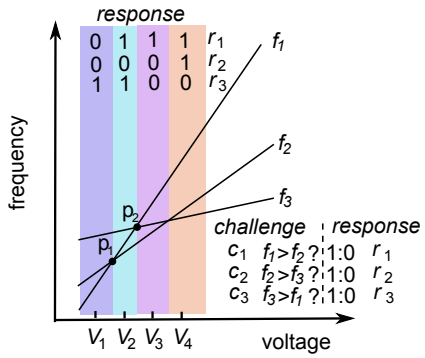

Figure 3. The selected unreliable response bits r_1, r_2, and r_3 applied to a specific ROPUF instance is not only dependent on the corresponding challenges c_1, c_2, and c_3, but is also a function of the supply voltages quantified by V_1, V_2, V_3 and V_4. Note that in an ROPUF, a challenge bit c selects a pair of ROs, and the response bit r is generated according to the comparison of frequencies of these two selected ROs.

will be highly unstable due to the predominant impact from measurement noise—this is alike to the metastable response produced from an Arbiter PUF given certain challenges [23]. However, if the supply voltage shifts to another point, the regeneration of r_3 becomes stable. For example, when r_3 is regenerated at the voltage V_1, it consistently results in '1'. Similarly, it consistently produces '0' when it is evaluated at the voltage of V_4.

If we evaluate the reliability of r_3 across a wide range of supply voltages, we can see that r_3 is unstable because it flips when the supply voltage shifts from V_1 to V_4. In conventional PUF applications, it is undesirable that f_1 and f_3 intersects within a range of operating conditions, eg., between V_1 and V_4 at the crosspoint p_2. However, in the construction of a PUF sensor, such phenomena is desired because of the sensitivity of the response to environmental parameters—in this case supply voltage—that can eventually be used to discover the PQ value hidden in a response vector.

Unreliable response bits in a circuit based PUF, such as the ROPUF, strongly depend on the *supply voltage* given the same challenge. Inspired by the foregoing observation, we expect that unreliable response bits can be successfully exploited to recover the voltage applied to a PUF. For instance, in Fig. 3, if the response $\mathbf{R}$ for the given challenge $\mathbf{C}$ is '001', then the voltage is approximately derived as V_1.

IV. Validation with ROPUFs

We use an ROPUF implementation for validating the proposed PUF sensor concept to demonstrate that voltage can indeed serve as a versatile PQ since existing transducers for sensing can server as the source of supply voltage variations. We use the ROPUF experimental data in [24] consisting of five ROPUFs implemented across five Spartan3E S500 FPGAs. Each FPGA consists of 512 ROs to form a ROPUF. Detailed implementation information can be found in [24]. For a given challenge, the response is reproduced under 0.96 V, 1.08 V, 1.20 V, 1.32 V and 1.44 V respectively, under the operating temperature of 25°C. Each response to a given challenge is evaluated 100 times under a given operating condition. We begin by providing two definitions to ease the following discussion and evaluation.

Definition 1. InterPQ-distance. The interPQ-distance is a random variable describing the distance between two PUF responses $\mathbf{R}^{\text{PQ}_1}, \mathbf{R}^{\text{PQ}_2}$ produced under different PQs by applying the same challenge to the same PUF sensor, hence,

$$D_{\text{interPQ}} = \text{dist}(\mathbf{R}^{\text{PQ}_1}, \mathbf{R}^{\text{PQ}_2}) \tag{1}$$

where $\mathbf{R}^{\text{PQ}_1}, \mathbf{R}^{\text{PQ}_2}$ are two responses generated under two random and distinct PQs by applying the same challenge to the same PUF sensor.

Definition 2. IntraPQ-distance. The intraPQ-distance is a random variable describing the distance between two PUF responses $\mathbf{R}^{\text{PQ}}, \mathbf{R}^{\text{PQ}'}$ from the same PUF sensor and using the same challenge under the same PQ setting.

$$D_{\text{intraPQ}} = \text{dist}(\mathbf{R}^{\text{PQ}}, \mathbf{R}^{\text{PQ}'}) \tag{2}$$

where $\mathbf{R}^{\mathrm{PQ}}, \mathbf{R}^{\mathrm{PQ}'}$ are two randomly re-evaluated responses from a randomly chosen PUF sensor by using the same challenge under the same PQ setting.

The dist(.;.) can be any well-defined and appropriate distance metric over the responses. In this paper, responses are always bit vectors and the distance metric used is Hamming distance (HD) or fractional Hamming distance (FHD).

Readers who are familiar with PUFs will notice that the definition of the interPQ-distance is similar to the inter-distance of PUFs that measures the difference between two responses from two distinct PUF instances given the same challenge. The difference is that the InterPQ-distance is evaluated across differing PQ values, still referred to the same PUF instance. Whereas the IntraPQ-distance is similar to the intra-distance of PUF responses that measures the difference between two responses reproduced by two random and distinct evaluations by applying the same challenge to the same randomly chosen PUF instance. The main difference is that the intra-distance does not consider the source of the PQs, it treats any PQ as a noise source. However, we only treat the unwanted PQs as noise sources. In our case temperature is a noise source but voltage is not. Similar to the inter-distance and intra-distance distribution [22], both the interPQ-distance and intra-distance can be assumed to follow a binomial distribution $B(n,p)$. The binomial probability estimator of interPQ-distance and intraPQ-distance distributions are $\hat{p}_{\mathrm{interPQ}}$ and $\hat{p}_{\mathrm{intraPQ}}$, respectively. As in [22], the $\hat{p}_{\mathrm{interPQ}}$, in general, is the probability of $\mathbf{R}^{\mathrm{PQ}_1} \neq \mathbf{R}^{\mathrm{PQ}_2}$, see definition 1, the $\hat{p}_{\mathrm{intraPQ}}$ is the probability of $\mathbf{R}^{\mathrm{PQ}} \neq \mathbf{R}^{\mathrm{PQ}'}$, see definition 2.

To increase the capability of correctly distinguishing different sensed PQ values, it is imperative to have a set of challenges with a lower $\hat{p}_{\mathrm{intraPQ}}$ and higher $\hat{p}_{\mathrm{interPQ}}$—as detailed in Section IV-B. Alternatively, given that only challenges that generate unreliable response bits, discarded in conventional PUF applications, contribute to sensing capability of the PUF sensor, having the ability to select such challenges for secure sensing can greatly ease the recovery of a PQ value. Therefore, we propose a methodology to pre-select challenges with response bits more likely to be sensitive environmental factors to increase the resulting difference between $\hat{p}_{\mathrm{intraPQ}}$ and $\hat{p}_{\mathrm{interPQ}}$.

A. Selecting Challenges Sensitive to a PQ

In Fig. 3, if the ROs oscillation frequencies of f_1 and f_2 do not intersect within a specific operating voltage range, specifically, between 0.96 V to 1.44 V with respect to the employed ROPUF sensor, then the regeneration of response bits r_1 upon frequency comparison is always consistent and shows strong tolerance to voltage deviations. In such cases, these challenges leading to stable response bits cannot be employed to sense the operating voltage because they are incapable of reflecting voltage changes. Therefore, it is more efficient to pre-select challenges leading to unreliable response bits—referred to from henceforth as simply *unreliable challenges*—that are affected by changes in operating voltage and employ them to discover the voltage and the veracity of the measurement. We will show in Section IV-B that the unreliable challenge selection strategy is indeed a more efficient approach to recover a hidden PQ value from PUF sensor responses.

For ROPUFs, we can pre-select the unreliable challenge based on the frequency difference Δf among ROs. If such a frequency difference is small among different ROs, response bits generated upon them are likely to be different with high probability when the voltage changes. This is the foundation of our proposed PUF sensor. Fig. 4 illustrates the frequency distribution of 512 ROs under an operating voltage of 1.20 V, which is the nominal or reference voltage for the measurements. The mean value is 197.8 MHz. If we select ROs satisfying $|f - 197.8\ \mathrm{MHz}| < \Delta f$ for response generation, it is clear that the number of ROs selected is related to the setting of Δf. The number will increase as Δf becomes larger.

As we mentioned in Section IV, it is desirable to increase the difference between $\hat{p}_{\mathrm{interPQ}}$—PQ is voltage in this specific experimental validation—and $\hat{p}_{\mathrm{intraPQ}}$. A larger difference between $\hat{p}_{\mathrm{interPQ}}$ and $\hat{p}_{\mathrm{intraPQ}}$ will facilitate the recovery of the measured PQ. The relationship between the difference of $\hat{p}_{\mathrm{interPQ}}$ and $\hat{p}_{\mathrm{intraPQ}}$ and the setting of Δf is shown in Fig. 5. We can see that the difference is significantly increased from less than 10% to more than 30% when the Δf reduces. Fig. 6 shows the $\hat{p}_{\mathrm{intraPQ}}$ and $\hat{p}_{\mathrm{interPQ}}$ of five different ROPUFs across five FPGA boards. We can see that the difference between $\hat{p}_{\mathrm{intraPQ}}$ and $\hat{p}_{\mathrm{interPQ}}$ is large enough to distinguish $V_i = 1.2$ V, where $V_i \in \{0.96\ \mathrm{V}, 1.08\ \mathrm{V}, 1.20\ \mathrm{V}, 1.32\ \mathrm{V}, 1.44\ \mathrm{V}\}$, from $V_i = 1.32$ V. We will detail and quantify this in Section IV-B.

Note that, as highlited in Section IV-B, the user or verifier in the enrolment phase is able to obtain the RO frequencies directly from the counters through direct access that is disabled/destroyed once the enrolment phase is completed [25].

B. Secure Sensing Capability

The recovery of a PQ value from the responses of a PUF sensor involves two phase: i) enrolment phase; and ii) sensing phase.

In the enrolment phase or prior to comissioning a PUF sensor, a legitimate user is able to conduct measurements to accurately characterise the PUF sensor. In the case of ROPUFs, a user is able to measure frequencies of ROs directly from

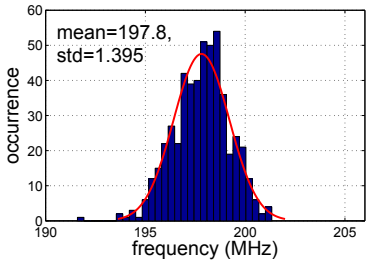

Figure 4. Frequency distribution of 512 ring oscillators (ROs) in one ROPUF.

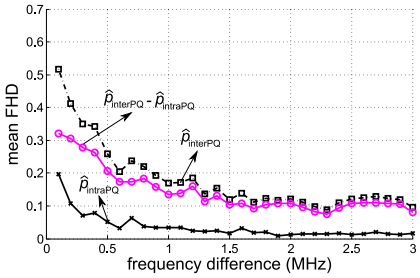

Figure 5. The $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$ as a function of different Δf—frequency difference—settings evaluated for one ROPUF. Unreliable challenge selection is performed under the reference voltage of 1.20 V and $\hat{p}_{\text{intraPQ}}$ is evaluated under 1.20 V

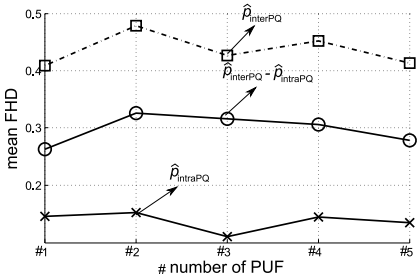

Figure 6. $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$ evaluated across five ROPUFs. Unreliable challenge selection is performed under the reference voltage of 1.20 V, $\hat{p}_{\text{intraPQ}}$ is evaluated under 1.32 V and Δf is set to be 0.3 MHz.

the counter. This direct access is disabled/destroyed once the enrolment phase is completed [25] to prevent an adversary from gaining measurements to characterise the PUF sensor to the same degree as the legitimate user or verifier. The one-time measurements thus obtained can subsequently be used by the verifier to generate challenge-response pairs (CRPs) or to pre-select unreliable challenges or both. In general, an accurate characterisation of a PUF sensor through one-time privileged access can provide a means to generate challenge-response pairs (CRPs) under different PQ values [26], [27]. Alternatively CRPs can be collected through applying the same challenges to the same PUF sensor under different PQ values. These CRPs are securely stored or generated on demand using prior characterisation of a PUF sensor. During the sensing phase, the PQ values are recovered by comparing the received responses with the enrolled responses given the same challenges.

Suppose the user compares each recorded response $\mathbf{R}^{\text{PQ}_\text{j}}$, $j \in \{1, ..., p\}$—obtained under PQ_j to the challenge $\mathbf{C}$—with the received response $\mathbf{R}^{\text{PQ}_\text{i}}$. Only the response $\mathbf{R}^{\text{PQ}_\text{j}}$, where $i = j$, held by the verifier will match the received response $\mathbf{R}^{\text{PQ}_\text{i}}$ given the same queried challenge $\mathbf{C}$. If the user finds that one of the responses $\mathbf{R}^{\text{PQ}_\text{j}}$ matches the received $\mathbf{R}^{\text{PQ}_\text{i}}$, then the sensed value of PQ_i is discovered. Otherwise, this received value is rejected.

Clearly one single CRP is not able to correctly recover a specific PQ in the field. Further, the strict matching of response bits is not practicable due to response unreliability caused by other factors such as temperature. Therefore, suppose the

Table I
QUANTITATIVE EVALUATION OF SENSING CAPABILITY UNDER DIFFERENT $\hat{p}_{\text{interPQ}}$ AND $\hat{p}_{\text{intraPQ}}$ THAT ARE DETERMINED BY Δf.

			EER $< 10^{-6}$			
Δf MHz	$\hat{p}_{\text{intraPQ}}$	$\hat{p}_{\text{interPQ}}$	n	n_{EER}	FAR*	FRR*
3	1.62%	9.68%	623	29	−6.00	−6.27
2	1.34%	12.04%	380	19	−6.03	−6.04
1	3.48%	16.88%	397	35	−6.03	−6.10
0.5	5.21%	25.80%	244	33	−6.01	−6.21
0.3	7.16%	31.00%	167	31	−6.04	−6.02

Note: the * symbol indicates $\log_{10}(\cdot)$ of the value.

recovery of a PQ value is based on the number of differing response bits being less than or equal to a threshold n_{th}. This leads two error rates: false acceptance rate (FAR) and false rejection rate (FRR). FAR stands for the probability of a user incorrectly recovering a PQ_j instead of the authentic PQ_i, $i \neq j$. While FRR stands for the probability of the authentic PQ_i being falsely rejected. Now, sensing capability can be evaluated by the probability of correctly recovering a specific PQ value, such as 1.2 V, through the evaluation of a number of CRPs where it is imperative to ensure both FAR and FRR are minimized in practice to be successful.

When the length of response bits or the number of CRPs, n, and the threshold n_{th} used to evaluate a response and recover a PQ value are given, then the FAR and FRR can be formally expressed following work in [22], [28]:

$$\text{FRR} = 1 - \sum_{i=0}^{n_{\text{th}}} \binom{n}{i} (\hat{p}_{\text{intraPQ}})^i (1 - \hat{p}_{\text{intraPQ}})^{(n-i)}, \quad (3)$$

$$\text{FAR} = \sum_{i=0}^{n_{\text{th}}} \binom{n}{i} (\hat{p}_{\text{interPQ}})^i (1 - \hat{p}_{\text{interPQ}})^{(n-i)}. \quad (4)$$

There exists a threshold value to make both FAR and FRR equal. We refer this interested threshold value as *equal error threshold*, termed as n_{EER}. Consequentially, when both error rates are equal, we refer this equal rate as *equal error rate* (EER) following Roel's work [22]. For a discrete distribution, there may not be an n_{EER} for which FAR is equal to FRR, and in that case, n_{EER} and EER are defined as in [22]:

$$n_{\text{EER}} = \underset{n_{\text{th}}}{\text{argmin}} \{\max\{\text{FAR}(n_{\text{th}}), \text{FRR}(n_{\text{th}})\}\}, \quad (5)$$

$$\text{EER} = \max\{\text{FAR}(n_{\text{EER}}), \text{FRR}(n_{\text{EER}})\}. \quad (6)$$

In Table. I, we show quantitative evaluations of n—minimal number of challenges needed to meet the EER, and n_{EER} of PUF sensors under different $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$. Recall that both $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$ are influenced by the chosen Δf as shown in Fig. 5 and the PQ in this table is voltage. We can see from Table. I, the necessary bit length or number of challenges n decreases as Δf is reduced. This indicates the efficiency of implementing the proposed unreliable challenge selection method.

V. Conclusion

We take advantage of unreliable response bits of conventional PUFs to investigate a PUF sensor framework where operating voltage measurements are hidden in PUF responses. The capability of the PUF sensor to sense an electrical signal—the voltage—leads to a potential universal PUF sensor architecture when other PQs can be converted to a voltage through a transducer. Moreover, we proposed a method of selecting challenges that generate unreliable response bits to improve the sensing capability by exploiting challenges that are more sensitive to voltage variations. Based on experimental data, we quantify the sensing capability.

Further work is required to address several challenges: i) to increase the resolution of sensing and avoid employing a larger number of CRPs, n, the sensitivity of responses to the PQ needs to be amplified; ii) further improving $\hat{p}_{\mathrm{intraPQ}}$ by reducing the influence from unwanted PQs is desirabale and may be achieved by PUF designs invariant to temperature changes [29], more specificly, from $-20^{\circ}\mathrm{C}$ to $120^{\circ}\mathrm{C}$; and iii) a lightweight protocol that can be eomployed with a PUF sensor should be developed and may be built upon a strong PUF [21], [30] or a reverse/reusable fuzzy extractor [31], [32] to prevent model building attacks.

Acknowledgment

This research was supported by the Australian Research Council Discovery Program (DP140103448). We acknowledge support from China Scholarship Council (201306070017).

References

[1] T. S. López, D. C. Ranasinghe, M. Harrison, and D. McFarlane, "Adding sense to the Internet of Things," *Personal and Ubiquitous Computing*, vol. 16, no. 3, pp. 291–308, 2012.

[2] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi, and G. Tsudik, "Invited-things, trouble, trust: on building trust in IoT systems," in *Proc. Design Automation Conf. (DAC)*, 2016, p. 121.

[3] D. C. Ranasinghe, K. S. Leong, M. L. Ng, D. W. Engels, and P. Cole, "A distributed architecture for a ubiquitous RFID sensing network," in *Proc. Int. Conf. Intelligent Sensors, Sensor Networks and Information Processing*, 2005, pp. 7–12.

[4] R. Torrance and D. James, "The state-of-the-art in IC reverse engineering," in *Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 2009, pp. 363–381.

[5] B. Gassend, D. Lim, D. Clarke, M. Van Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 11, pp. 1077–1098, 2004.

[6] D. C. Ranasinghe and P. H. Cole, "Confronting security and privacy threats in modern RFID systems," in *Proc. Fortieth Asilomar Conf. Signals, Systems and Computers*, 2004, pp. 2058–2064.

[7] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. Design Automation Conf. (DAC)*, 2007, pp. 9–14.

[8] A. B. Alvarez, W. Zhao, and M. Alioto, "Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fj/bit in 65 nm," *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, 2016.

[9] R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2012, pp. 302–319.

[10] Y. Gao, G. Li, H. Ma, S. F. Al-Sarawi, O. Kavehei, D. Abbott, and D. C. Ranasinghe, "Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices," in *Proc. Int. Conf. Pervasive Computing and Communication (Percom) Workshops*, 2016, pp. 1–6.

[11] D. Lim, "Extracting secret keys from integrated circuits," Master's thesis, Massachusetts Institute of Technology, 2004.

[12] U. Ruhrmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, 2013.

[13] G. T. Becker, "The gap between promise and reality: On the insecurity of XOR Arbiter PUFs," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2015, pp. 535–555.

[14] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *Proc. IEEE. Int. Symp. Hardware Oriented Hardware-Oriented Security and Trust (HOST)*, 2010, pp. 112–117.

[15] J. Rajendran, J. Tang, and R. Karri, "Securing pressure measurements using sensorpufs," in *Proc. IEEE Int. Symp. Circuits and Systems (ISCAS)*, 2016, pp. 1330–1333.

[16] U. Rührmair, J. Martinez-Hurtado, X. Xu, C. Kraeh, C. Hilgers, D. Kononchuk, J. J. Finley, and W. P. Burleson, "Virtual proofs of reality and their physical implementation," in *Proc. IEEE Symp. Security and Privacy (S&P)*, 2015, pp. 70–85.

[17] U. Ruehrmair, M. Stutzmann, J. Finley, C. Jirauschek, G. Csaba, P. Lugli, E. Biebl, R. Dietmueller, K. Mueller, and H. Langhuth, "Method for security purposes," Sep. 30 2011, US Patent App. 13/250,534.

[18] B. Fisch, D. Freund, and M. Naor, "Physical zero-knowledge proofs of physical properties," in *Advances in Cryptology (CRYPTO)*, 2014, pp. 313–336.

[19] S. Katzenbeisser, Ü. Kocabaş, V. Van Der Leest, A.-R. Sadeghi, G.-J. Schrijen, and C. Wachsmann, "Recyclable PUFs: Logically reconfigurable PUFs," *Journal of Cryptographic Engineering*, vol. 1, no. 3, pp. 177–186, 2011.

[20] S. Sharif Mansouri and E. Dubrova, "Ring oscillator physical unclonable function with multi level supply voltages," in *Proc. Int. Conf. Computer Design (ICCD)*, 2012, pp. 520–521.

[21] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Memristive crypto primitive for building highly secure physical unclonable functions," *Scientific Reports*, vol. 5, art. no. 12785, 2015.

[22] M. Roel, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, Ph. D. thesis, Dissertation, University of KU Leuven, 2012.

[23] D. C. Ranasinghe, D. Lim, S. Devadas, D. Abbott, and P. H. Cole, "Random numbers from metastability and thermal noise," *Electronics Letters*, vol. 41, no. 16, p. 1, 2005.

[24] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardware-Oriented Security and Trust (HOST)*, 2010, pp. 94–99.

[25] M.-D. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A lockdown technique to prevent machine learning on PUFs for lightweight authentication," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 146–159, 2016.

[26] R. Maes, "An accurate probabilistic reliability model for silicon PUFs," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2013, pp. 73–89.

[27] T. Xu, D. Li, and M. Potkonjak, "Adaptive characterization and emulation of delay-based physical unclonable functions using statistical models," in *Proc. Design Automation Conf. (DAC)*. ACM, 2015, p. 76.

[28] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, 2005.

[29] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 7, pp. 1143–1147, 2015.

[30] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," IEEE Access, vol. 4, pp. 61–80, 2016.

[31] A. Van Herrewege, S. Katzenbeisser, R. Maes, R. Peeters, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," in *Financial Cryptography and Data Security*. Springer, 2012, pp. 374–389.

[32] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith, "Reusable fuzzy extractors for low-entropy distributions," in *Proc. Int. Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. Springer, 2016, pp. 117–146.