PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing

Yansong Gao, *Student Member, IEEE*, Hua Ma, Derek Abbott, *Fellow, IEEE*, and Said F. Al-Sarawi, *Member, IEEE*

***Abstract*— Wireless sensors are increasingly penetrating every domain of our lives through integration with Internet of Things, e.g., such devices are widely incorporated into smart buildings and for monitoring critical industrial infrastructure. Sensing, collecting and communication of sensor data, however, are under threat from various attacks due to the difficulty in implementing proper protection mechanisms and limited computational resources available in these cost-sensitive devices. This paper expands on recent research on physical unclonable function (PUF) sensors to secure sensing by taking the advantage of inherent physical randomness. In particular, PUF unreliability originates from its sensitivity to ambient parameter variations that is usually undesirable for elementary PUF applications—such as authentication and key generation—is exploited to guarantee the veracity of the sensed value. In this paper, a PUF naturally acting as a sensor or a PUF explicitly integrated with a sensor is called a PUF sensor. Security of sensing in a PUF sensor is attributed to the natural merging of cryptography and sensing to eschew the need for a standalone crypto module. Thus, the PUF sensor is appealing for low-cost applications. To obtain the sensed value, we develop an authenticated sensing protocol that is robust against eavesdropping, also capable of detecting man-in-the-middle manipulation of the sensed value. Compared to initial investigations of PUF sensors, we avoid the stringent requirements of a strong PUF. We validate the feasibility of the proposed authenticated sensing protocol based on an experimental implementation of a ring oscillator PUF sensor. To improve the sensing capability, we present an efficient approach to select sensitive responses and only employ them for sensing. Significantly improved efficacy is validated through comprehensive experimental results.**

***Index Terms*— PUF sensor, wireless sensing, hardware security, replaying attack, data manipulation.**

I. Introduction

OVER the last decade, our daily lives have continually benefited from the wide deployment of smart devices. We are entering into the Internet of Things (IoT) era, where smart devices are connected and interact with each other. Sensors are tentacles of the network of interconnected IoT devices and responsible for sensing the environment, collecting and communicating sensed data [1]. Due to the ubiquity of these sensors and the physical exposure when they are deployed in the (malicious) field, sensors are easy to attack. Note that IoT devices are often deployed in security and privacy critical application scenarios such as e-health, smart-homes, critical public infrastructure monitoring, etc. Thus, it is paramount to guarantee the veracity of sensing and detect malicious man-in-the-middle attacks that utilize insecure communication channels. Unlike high-end computing devices, IoT devices are usually limited in area and power budget. Therefore, a traditional cryptographic solution that relies on a separate crypto module is naturally less attractive for these resource-constrained devices. Further, costly crypto modules conflict with the cost-sensitive feature of widely distributed sensors [2]. On the other hand, security of cryptographic algorithms relies on digital secret keys stored in non-volatile memory (NVM) that is assumed untouchable or unbreakable. Such an assumption, in practice, cannot hold as digital secret keys within NVM can be extracted under a variety of attacks including non-invasive, semi-invasive and invasive attacks [3].

Since the advent of silicon based Arbiter PUFs (APUFs) [4], PUFs witnessed a wide range of applications and became inseparable trust anchors of resource-constrained devices [5]–[7]. Generally, a PUF is analogous to a fingerprint that is created upon the fabrication of a hardware device by exploiting imperfections or uncertainties within a manufacturing process. Two identical PUFs are impossible to be forged even by the same producer. On one side, a PUF is a physical function that reacts with an instance-specific response (output) when it is queried by a challenge (input). Notably, a PUF usually has more than one challenge response pairs (CRPs). Different PUF instances exhibit significantly varying responses for the same challenge. Thus, PUF integrated devices are able to be uniquely distinguished based on instance-specific CRP behaviors. On the other side, given the same PUF, the same response is expected to be regenerated whenever the same challenge is presented. However, in practice, response regeneration is prone to changes in operating conditions such as voltage and temperature. Note that PUFs have two primary applications: key generation and authentication. Key generation requires a highly stable response [8], thus, it is imperative to improve PUF reliability and correct those potential response errors

Manuscript received December 7, 2016; revised April 1, 2017 and April 10, 2017; accepted April 13, 2017. Date of publication May 15, 2017; date of current version August 28, 2017. This work was supported in part by the Department of State Development, Collaboration Pathways Program, Government of South Australia, under Grant CPP39, and in part by the China Scholarship Council under Grant 201306070017. This paper was recommended by Associate Editor M. Alioto. *(Corresponding author: Yansong Gao.)*

Y. Gao, D. Abbott, and S. F. Al-Sarawi are with the School of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA 5005, Australia (e-mail: yansong.gao@adelaide.edu.au; derek.abbott@adelaide.edu.au; said.alsarawi@adelaide.edu.au).

H. Ma is with the Auto-ID Labs, School of Computer Science, The University of Adelaide, Adelaide, SA 5005, Australia (e-mail: mary.ma@adelaide.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2017.2695228

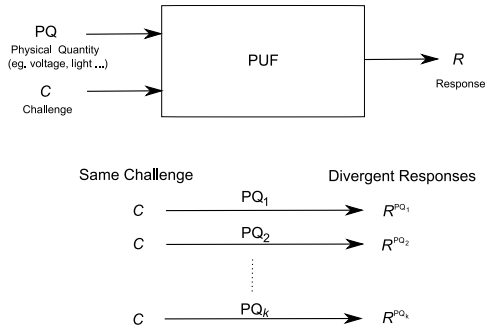

Fig. 1. PUF as a sensor. The response is determined by both the PQ and the queried challenge.

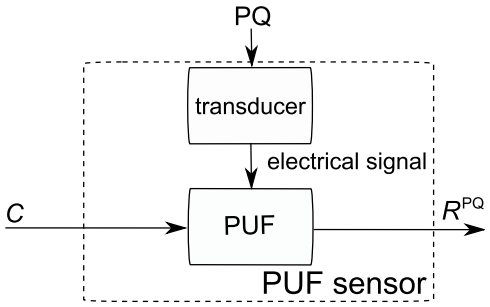

Fig. 2. A universal PUF sensor architecture. It exploits inherent response sensitivity to the electrical signal—voltage or current that are interchangeable. Voltage is used for descriptions and validations in this work. Other PQs can be converted into voltage by an on-chip transducer.

prior to extracting a key. In PUF CRP-enabled authentication applications [6], [9], it is preferable to maximize the response reliability i) to increase the ability of distinguishing one PUF instance from a large PUF population ii) and to increase the difficulty in carrying out the modeling attacks [10]–[13].

Similar to the philosophy of exploiting undesirable manufacturing randomness to build a PUF that acts as a fingerprint, we further take advantage of inherent PUF response unreliability to ambient environment parameters to sense these parameters. The line of investigation, building on the new PUF sensor paradigm, is put forward by Rosenfeld *et al.* [2] and has gained significant attention in recent years [14]–[17], where a PUF is employed to secure sensing by making use of inherent physical randomness rather than reliance on traditional cryptographic operations based on a standalone crypto module [18]. In this context, the PUF presents itself as a sensor to sense a particular physical quantity (PQ)—an environmental parameter [2]. The natural merging of cryptography with sensing is promising for defeating the most vexing attack on sensors—sensor node capture attack, where an attacker has physical access to a sensor node, extracting the digital secret key, modifying the programming, or simply replacing it with a malicious node [19]. The PUF sensor mitigates such an attack since there is no digital key involved. Replacing a PUF sensor is non-trivial due to the PUF sensor's unclonability. In contrast to traditional PUF applications that there is only one input (challenge), the PUF sensor takes two inputs: one is the challenge and the other is the PQ of interest, as generalized in Fig. 1.

A PUF sensor can be mathematically abstracted as a hash function $\text{Hash}_K(\mathbf{C}, \text{PQ})$. For a given PQ value, there are different outputs of $\text{Hash}_K(\mathbf{C}, \text{PQ})$ when the challenge $\mathbf{C}$ is different. The principle is that every $\mathbf{C}$ gives a PQ-specific hash output. By knowing the specific hash output corresponding to a challenge $\mathbf{C}$, it is possible to discover the PQ value. Notably, $\text{Hash}_K(\mathbf{C}, \text{PQ})$ is inherently endowed by the manufacturing randomness. Therefore, the hash is an instance-specific function, if an attack is possible on $\text{Hash}_K(\mathbf{C}, \text{PQ})_A$, the gained information from this attack will not provide extra information that makes it easy to mount attach on another $\text{Hash}_K(\mathbf{C}, \text{PQ})_B$.

This paper expands on previous research [2], [14]–[17] and investigates several important yet unexplored aspects. We formalize PUF sensor properties and examine the practicability of achieving these properties. An authenticated sensing protocol applicable to PUF sensors is developed to recover sensed PQ values by exploiting the behavior of unreliable response bits that are sensitive to the PQ. The protocol is able to automatically detect malignant man-in-the-middle tampering of sensed values, and hence, defeat veracity spoofing without requiring a trusted communication channel. We attempt to eliminate the strict requirement of a strong PUF to realize a secure protocol. Without a strong PUF, the PUF sensors conceptualized in [2] and [16] have difficulty in preventing manipulation of sensed measurements when the communication channel is insecure. This is because the PUF sensor [2], [16] is a weak PUF [12] with a limited CRP space. In addition, compared to previous studies [2], [14], instead of only sensing a specific PQ, e.g., temperature [14], light luminosity [2], or pressure [16], converting these parameters into an electrical signal—e.g., voltage or current—is more appealing, since the chosen electrical parameter is versatile. Various types of PQs such as temperature, humidity, sound energy, can eventually be converted into electrical signals through a transducer to influence the reliability of a PUF. The PUF sensor architecture is illustrated in Fig. 2. In this approach, other PQs are able to be securely sensed indirectly through the corresponding electrical signal. Hence a PUF sensor that is capable of securely sensing electrical signals—specifically, this work uses the voltage for validation—can possibly as a *universal* PUF sensor. We validate the proposed authenticated sensing protocol using a ring oscillator PUF (ROPUF) sensor to correctly find voltage values to potentially serve as a *universal* PUF sensor. Moreover, we present a simple, yet efficient approach, that is applicable to ROPUFs to expedite the selection of unreliable response bits that are highly sensitive to voltage variations. Comprehensive quantitative evaluations are used to validate the significantly improved sensing capability by only employing these sensitive responses.

The rest of the paper is organized as follows. Background and related work are introduced in Section II. In Section III, we formalize the PUF sensor properties, and present an ROPUF sensor implementation to detail the principles of exploiting the PUF unreliability for sensing. Then comprehensive experimental validations are carried out in Section IV after we present an efficient sensitive response selection approach

in order to improve the sensing capability. Discussion of the security of the sensing methodology is presented in Section V. In Section VI, we conclude this work and discuss several challenges of realizing a more efficient PUF sensor.

II. Background and Related Work

A. Background

A PUF primitive was first proposed by Pappu *et al.* in 2001 [20], [21]. The implementation is an optical PUF, initially dubbed a physical one-way function. The response (speckle pattern) is dependent on the input laser location/polarization (challenge) when the laser irradiates a stationary scattering medium. The optical PUF is mainly limited by its hardness to be integrated with current tiny electronic components and the complicated challenge response evaluation procedures that require careful calibrations.

Following this prototype PUF, a practical implementation of a silicon based PUF initially called a Physical Random Function, later termed the Arbiter PUF (APUF), was proposed by Gassend *et al.* [4], which exploits manufacturing variability in gate and wire delays as the source of unclonable randomness. The response is generated based on the time delay difference between two signal propagation paths consisting of serially connected electronic cells, e.g., multiplexers. The path through each cell is determined by a selection bit in a challenge vector [22]. This structure is simple, compact and capable of generating an exponential number CRPs.

An APUF is prone to metastability when the delay difference between two paths is close to zero when given a certain challenge, due to a racing condition between the two paths. Because the arbiter, e.g., a latch, is incapable of definitely determining the winning signal path due to the inability of such gates to resolve a small time difference. An ROPUF was proposed [6] to mitigate the above issues of the APUF. Some studies have improved the number of CRPs available from an ROPUF [23], [24] and increased its resilience to modeling attacks [23]. A survey of ROPUFs can be found in [25].

Besides the aforementioned delay-based PUFs, there are mismatch based silicon PUFs such as the SRAM PUF [26], [27], latch PUF [28], flip-flop PUF [29], [30], butterfly PUF [31], Anderson PUF [32] and analog PUFs. The later one has other variants such as the current-based PUF [33] and nonlinear current mirror based PUF [34]. There are also other PUF designs that exploit electronic circuits properties such as static nonlinearities of data converters [35] and switched-capacitors [36]. Comprehensive reviews of conventional PUF designs can be found in [37] and [38]. In recent years, emerging PUFs with nanotechnology are utilized to build PUFs beyond the aforementioned conventional silicon PUFs by taking advantage of prevalent process variations as a consequence of minimum feature size scaling to the nano region, and other unique properties offered in emerging nanoelectronics devices [39]–[43]. A survey of such nano PUFs can be found in [44].

B. Related Work

The PUF sensor expands the applications of current PUF constructions, which is first conceived by Rosenfeld *et al.* [2] in 2010 to overcome the requirement of a separate crypto module that relies on conventional cryptographic algorithms to encrypt a sensed data. This line of investigation keeps prospering that has been receiving increased attention in recent years (after 2015) [2], [14]–[17]. In [2] and [16], light luminosity and pressure sensing are validated using simulation results. PUFs presented in [2] and [16] are weak PUFs that are limited with a small CRP space. Therefore, to prevent exhaustive CRP characterization by a malicious party—adversary—within a short time period to build a mathematical copy that can impersonate the CRP behavior of the original PUF sensor, a shared key is used to protect CRPs [2]. The purpose is mainly to prohibit replaying attacks. However, the deployment of a shared key evades the PUF sensor from a lightweight sensing application and, to some extent, contradicts initial motivations to overcome the need for a key stored in the NVM. Cao *et al.* experimentally demonstrated image sensor based PUFs that use slightly modified commercial CMOS image sensors [15]. Such an image sensor, in general, incorporates inherent signatures in every image taken by this imager, where the signature of each imager is extracted from dark current non-uniformity of fixed pattern noise resulting from manufacturing imperfections. We are not intending to design or invent a specific PUF sensor that is applicable to sense one particular PQ. Our work takes advantage of unwanted but inherent PUF response unreliability induced by versatile electrical signals in conventional PUFs to discover various PQ values when such a PQ is represented by an electrical signal—to be specific, voltage in this work, and consequently, influences the PUF response behavior.

Rührmair *et al.* [14] and [45] examined the PUF sensor and experimentally demonstrated *virtual proof of reality* (VP)—a security concept complementary to physical zero-knowledge protocols [46]—that assures the proof of a physical statement, specifically, the temperature and distance between two objects, over an untrusted digital communication channel from the prover to the verifier without cryptographic algorithms. In VP, a prover *first* claims a physical statement and then proves it to the verifier. This protocol prevents the spoofing of physical statements by employing strong PUFs [47]. In this paper, generally, we are aiming to provide a generic PUF sensor architecture to be universal by exploiting auxiliary PUF properties to be adaptable for sensing various PQs. In addition, we provide an alternative to eliminating the requirement of strong PUFs, thus, PUF sensors with a limited CRP space are able to be secure even in the face of replaying attacks and man-in-the-middle manipulations by employing a reverse/reusable fuzzy extractor [48].

In essence, a PUF sensor makes use of auxiliary physical effects to alter original challenge-response mapping relationship in a conventional PUF construction. Technically, it is akin to the concept of a reconfigurable PUF where external effects are used to reconfigure challenge-response behaviors [49]–[51]. Mansouri and Dubrova [51] used multiple supply voltage for reconfiguration purpose to alter the challenge-response pair behavior in order to increase the CRP space of an ROPUF. By contrast, we exploit the altered challenge-response behavior originated from voltage

fluctuations to recover the applied voltage for secure sensing purpose.

III. Secure Wireless Sensing Based on PUF Unreliability

Building upon the concepts articulated in [2], we formalize that a PUF sensor should have the following properties:

(a) PUF sensor's response is not only a function of a challenge, but also has a strong dependence on a particular PQ.
(b) Two identical PUF sensors cannot be forged.
(c) The response remains relatively stable for a given challenge subjected to the same PUF sensor and a given PQ value.
(d) Given a known response under a PQ value, it is infeasible to predict neither the response for the same challenge to a different PQ value, nor the response for the same PQ value to a different challenge.

In practice, a PUF sensor is able to satisfy above properties. The PUF response sensitivity to environmental parameters meets with the property (a). The inherent randomness resulted from manufacturing guarantees properties (b) and (d) attributing to the unpredictability of responses. The property in (d) is inherent to some PUFs such as SRAM PUFs [26], [27], [52] where CRP behaviors are independent with each other, proper but lightweight post-processing of the responses enables them suitable for PUF sensor applications as discussed in Section V even with a limited CRP space. For property (c), the PUF sensor responses are expected to be only sensitive to a specific PQ, e.g., voltage, but invariant to other PQs, e.g., temperature. This property can also be met, which is shown in Section V.

In the following, we detail the insights that inherent PUF unreliable response bits can be utilized to discover PQ—versatile voltage—values using a popular time-delay based PUF construction, ROPUF.

A. PUF Unreliable Response Bits

A PUF is a physical function that exploits analog randomness to extract instance-specific CRPs, the PUF response regeneration, thus, is affected by environmental parameter changes. It is noticed that the altered PUF response behavior is retrievable whenever the PUF response unreliability originates from ambient parameter changes. This is different from the altered PUF response behavior results from the thermal noise that is truly unexpected and unrepeatable. More specifically, same or similar response behavior is repeatable given *the same operating condition* subjected to the same challenge applied to the same PUF, though repeatedly evaluated responses do differ *across a range of operating conditions*. This insight is detailed by using an ROPUF in the following.

In general, an ROPUF has k identical ring oscillators (ROs), which ideally have the same oscillating frequency in the design phase. Notably, each RO consists of odd number of inverters to enable the self-oscillation whenever the power is up. In Fig. 3, we use three inverters in each RO as an example for simplicity purpose. The RO frequency is vulnerable to manufacturing randomness, thus, each RO has a unique frequency after fabrication. A challenge is fed into two multiplexers to select a pair

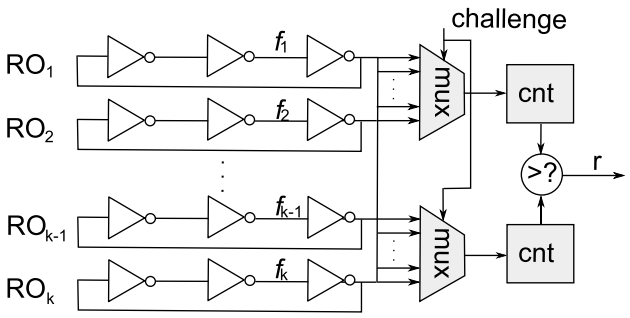

Fig. 3. Typical structure of a ring oscillator PUF (ROPUF).

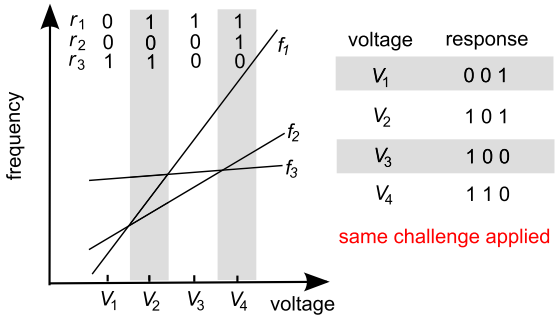

Fig. 4. Same challenge applied to the ROPUF leads to differing responses when the response is regenerated under a differing voltage. Those flipped reproduced PUF responses cause unreliability concern in conventional PUF applications such as authentication and key generation, but is desirable for PUF sensor. 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 chosen ROs. Specifically, c_1 selects f_1 and f_2, c_2 selects f_2 and f_3, c_3 selects f_3 and f_1. If the former RO's frequency is higher than the other one's frequency, response '1' is produced, otherwise, the corresponding response is '0'.

of ROs, RO_i and RO_j. Then frequencies f_i and f_j are counted given a fixed period by two counters and compared with each other using a comparator. The digital output, response, is determined by comparing frequencies of these two chosen ROs. For example, if $f_i < f_j$, then a response '0' is generated, otherwise, response '1' is given.

Besides inherent randomness introduced during manufacture, fluctuation of environmental parameters also influences the frequency of a given RO. Taking the voltage of interest into consideration, there exists an almost linear relationship between the RO's frequency and the applied voltage. The coefficient, corresponding to the relationship, however, varies from one RO to the other, which eventually results into the unreliability issue of the ROPUF when two ROs intersect within an operating range. Considering an example case as depicted in Fig. 4, the coefficient of RO_1 is higher than the coefficient of RO_3 because RO_1 oscillates faster than RO_3 when the supply voltage increases. As a consequence, the regenerated response r_3 flips from '1' to '0' as the voltage increases. The flipped response raises reliability concern because this induces negative effects in conventional PUF application such as authentication and key generation. In contrast, such a flipped response behavior is preferred for PUF sensors as only these unreliable responses exhibit sensitivity to environmental parameter changes that ultimately can be utilized for sensing

application. For those constantly reproduced responses, they are invariant to environmental parameter variations, thus is unable to be exploited for sensing. Notably, the 'unreliable' PUF response is still reproducible given the same challenge under the same PQ value, e.g., voltage. For example, the r_3 is constantly producing '1'/'0' when it is reevaluated under the voltage of V_1/V_4.

B. Sensing With Unreliable Response Bits

Unreliable response bits in a PUF strongly rely on the voltage given the same applied challenge. Inspired by the foregoing observations, unreliable response bits are exploited to recover the voltage applied to the PUF. For instance, in Fig. 4, if the response vector $\mathbf{R}$ given a challenge $\mathbf{C}$ is '101', then the voltage is derived as V_2. Then as well, if the response is '110', the voltage is V_4. Usage of a PUF sensor for sensing has following benefits:

(a) Overcoming the need for NVM to store digital keys and subsequent cryptographic operations to encrypt data.
(b) The response sent from the PUF sensor obfuscates sensed voltage value. But the trusted entity (the user) is able to recover the sensed value by observing the response.
(c) Man-in-the-middle tampering of the sensed data is detected and prevented. If the adversary does send a guessed or manipulated response to the user, the user is able to detect such a tampered response, thus, reject the sensed data.
(d) Replaying attacks are prevented. In this context, a challenge is used only once similar to a one-time-pad when a strong PUF is available or using a reverse fuzzy extractor allowing multiple usage of the same challenge to eliminate a strong PUF requirement.

In practice, the PQ can be any environmental parameters that are convertible to an electrical signal through a transducer. In this context, PQs, e.g., temperature, light luminosity, sound and humidity, can be sensed when they are represented by an electrical voltage signal that results in remapping of the unreliable response bits to a given set of challenges. As a consequence, fluctuation of these PQs can be converted into variations of the electrical signal, and thereupon be recovered by the unreliable response bits.

IV. ROPUF Sensors

ROPUF sensors are employed for experimental validations and the voltage is chosen as a versatile PQ where the voltage can be correctly sensed. Other PUF structures such as APUFs, SRAM PUFs can also be employed, since their responses are also sensitive to the electrical signal's variations. In this section, we firstly provide some preliminaries to ease the following descriptions. Considering that only unreliable response bits contribute to the sensing capability of a PUF sensor, employing more unreliable response bits can facilitate the developed authenticated sensing protocol. Hence, we develop a methodology of pre-selecting unreliable response bits of a ROPUF during the provisioning phase of the authenticated sensing protocol. Further, we quantitatively evaluate the developed sensing protocol's capability of correctly discovering the sensed PQ values based on comprehensive experimental results.

Due to the need for a number of ring oscillators and output frequencies to evaluate its response, the ROPUF is more power and area consuming in comparison with other popular PUF constructions such as SRAM PUFs and APUFs. The ROPUF power and area overhead can be reduced to 0.48 pJ and 39000 F^2 (F = min feature size) per bit based on the most recent ROPUF ASIC designs [7] implemented in 65 nm CMOS technology. The proposed PUF sensor kernel is not restricted to the ROPUF, instead the area and power efficient SRAM PUFs and APUFs can be used as well. The necessity and efficacy of i) selection of sensitive response bits—specific selection algorithm for other PUF structures may vary from the ROPUF presented in this work, and ii) the proposed sensing capability evaluation procedures validated using the ROPUF are applicable to other PUF structures.

A. Preliminaries

Definition 1 (InterPQ-Distance): The interPQ-distance is a random variable describing the distance between two PUF responses $\mathbf{R}^{\mathrm{PQ}_1}, \mathbf{R}^{\mathrm{PQ}_2}$ evaluated under different PQ values by querying the same challenge to the same PUF sensor, hence,

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

where $\mathbf{R}^{\mathrm{PQ}_1}, \mathbf{R}^{\mathrm{PQ}_2}$ are two responses evaluated under two random and distinct PQ values 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 $\mathbf{R}^{\mathrm{PQ}}, \mathbf{R}^{\mathrm{PQ}'}$ from the same PUF sensor and using the same challenge under the same PQ value.

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

where $\mathbf{R}^{\mathrm{PQ}}, \mathbf{R}^{\mathrm{PQ}'}$ are two responses obtained from a randomly chosen PUF sensor using the same randomly chosen challenge under the same PQ value.

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

Definition 3 (Hamming Distance): For bit vectors $\mathbf{X}_1$ and $\mathbf{X}_2$ with the same length l, the HD between them is defined as:

$$f_{\mathrm{HD}}(\mathbf{X}_1, \mathbf{X}_2) = \sum_{i=1}^{l} \mathbf{X}_1 \oplus \mathbf{X}_2. \tag{3}$$

Definition 4 (Fractional Hamming Distance): Built upon Eq. (3), the fractional Hamming distance (FHD) is defined as:

$$f_{\mathrm{FHD}}(\mathbf{X}_1, \mathbf{X}_2) = \frac{f_{\mathrm{HD}}(\mathbf{X}_1, \mathbf{X}_2)}{l}. \tag{4}$$

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 for the same PUF instance, but the inter-distance is evaluated across different PUF instances.

The intraPQ-distance is similar to the intra-distance of PUF responses that measures the difference between two responses reproduced by two 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 PQs, it simply treats all PQs as noise sources. However, in a PUF sensor, we only treat the unwanted PQs as noise sources. For example, in our study, temperature is noise source but voltage is not.

Similar to the inter-distance and intra-distance distribution of PUFs detailed in [37], both of the interPQ-distance and intraPQ-distance can be assumed to follow a binomial distribution $B(n, p)$. The binomial probability estimator of interPQ-distance and intraPQ-distance distributions are referred to as $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$, respectively. In general, the $\hat{p}_{\text{interPQ}}$ is the probability that $\mathbf{R}^{\text{PQ}_1} \neq \mathbf{R}^{\text{PQ}_2}$, see Definition 1, and the $\hat{p}_{\text{intraPQ}}$ is the probability that $\mathbf{R}^{\text{PQ}} \neq \mathbf{R}^{\text{PQ}'}$, see Definition 2.

To increase the capability of correctly distinguishing different PQ values when the authenticated sensing protocol—see Section IV-C—is implemented, it is imperative to increase the difference between $\hat{p}_{\text{intraPQ}}$ and $\hat{p}_{\text{interPQ}}$—elaborated in Section IV-D. Therefore, we first introduce the methodology of selecting unreliable response bits that are sensitive to the PQ to increase the difference between $\hat{p}_{\text{intraPQ}}$ and $\hat{p}_{\text{interPQ}}$.

B. Selecting Response Bit Sensitive to a PQ

We use the public experimental data from five ROPUFs implemented in five Spartan3E S500 FPGAs for validation of sensing the voltage. Each ROPUF consists of 512 ROs. We refer interested readers for detailed implementation information to [53]. The response is reevaluated under five discrete voltages, 0.96 V, 1.08 V, 1.20 V, 1.32 V and 1.44 V given the same challenge, all under the temperature of 25°C. Each response to a given challenge is evaluated 100 times under the same operating condition. We can see that $\binom{512}{2} = 130816$ response bits are available by comparing any two RO frequencies. Unfortunately, extraction of area and power overhead for the ROPUF sensor based on given set measurement data is not possible. Nonetheless, replacing the ROPUF with an APUF can provide a significant advantage in area and power. Thus an APUF implementation is an important open question for future study.

In Fig. 4, if the ROs oscillation frequencies of f_1 and f_2 do not intersect within an operating range, specifically, between 0.96 V to 1.44 V. Then the regeneration of response bit r_1 upon frequency comparison is always consistent and exhibits strong tolerance to voltage fluctuations. In such cases, these challenges leading to highly reproducible response bits are incapable of sensing the voltage due to the fact they are unable to reflect voltage changes. Therefore, it is necessary to pre-select unreliable challenges giving response bits that are sensitive to voltage changes and employ them to recover the voltage. This is more efficient, which will be experimentally validated in Section IV-D.

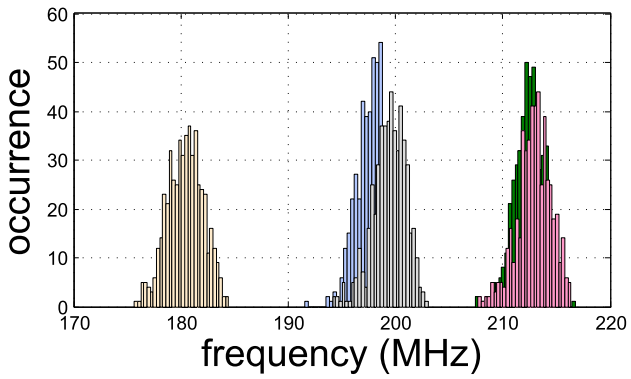

Fig. 5. Frequency distribution of 512 ROs for all five ROPUFs, it follows normal distribution. The RO frequencies are obtained under the operating condition of 1.2 V and 25°C.

Fig. 5 illustrates the frequency distribution of 5×512 ROs for all five ROPUFs under an operating voltage of 1.20 V. Noting that 1.20 V is the nominal or reference voltage for response evaluations. For each ROPUF, the RO's frequency follows normal distribution. Regarding to ROPUFs, we can pre-select the unreliable challenge that gives response sensitive to the PQ based on that the frequency difference Δf between two ROs is small. Only employing those selected sensitive response bits is the foundation of our proposed PUF sensor, whereas the sensitive response selection may vary from one PUF type to the other. The reason for selecting unreliable response bits under 1.20 V is that it is the central of different voltage settings—0.96 V, 1.08 V, 1.20 V, 1.32 V and 1.44 V. As for the ROPUF, the proposed response selection follows **Algorithm 1**. If the response is generated from a RO pair satisfying that the frequency difference between these two ROs is less than Δf, the response is selected. Otherwise, the response is discarded.

Algorithm 1 Selecting Sensitive Responses

```
procedure selection (frequencies of k ROs, Δf)
    for i = 1 : k − 1 do
        for j = 2 : k do
            if |f_i − f_j| < Δf then
                select this response based on comparison of f_i
                    and f_j;
            else
                this response based on comparison of f_i and f_j
                    is discarded;
            end if
        end for
    end for
end procedure
```

It is desirable to increase the difference between $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$—PQ is voltage in this specific experimental validation. A larger difference between $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$ will facilitate the recovery of the sensed PQ value. We will detail and quantify this in Section IV-D. The relationship between the difference of $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$ and the setting

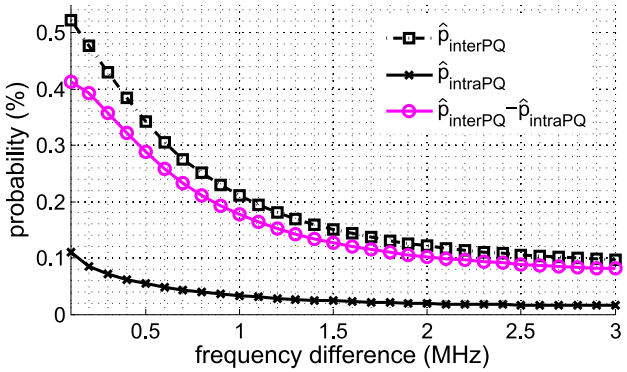

Fig. 6. The $\hat{p}_{interPQ}$ and $\hat{p}_{intraPQ}$ performance for one ROPUF to different Δf—frequency difference—settings. Unreliable response bits selection is performed under the reference voltage of 1.20 V. The $\hat{p}_{intraPQ}$ is evaluated under 1.20 V as well.

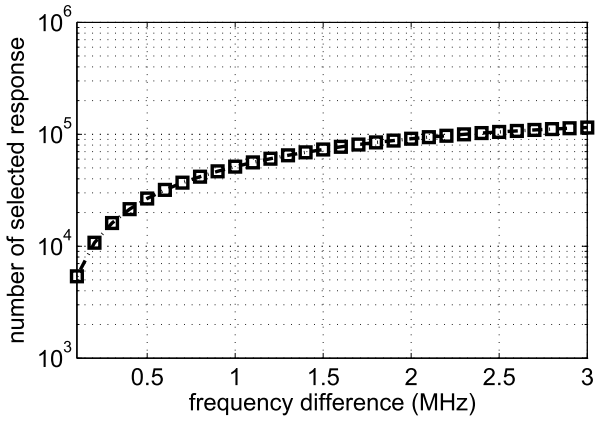

Fig. 7. Number of selected responses as a function of the Δf—frequency difference—settings. Smaller Δf, fewer number of selected responses, but higher sensitivity to the PQ.

of Δf is shown in Fig. 6. We can see that the difference is significantly increased from less than 10% to more than 40% when the Δf shrinks. As a consequence, the bit length of the response to successfully perform authenticated sensing will be significantly reduced—analyses of the required bit length of response for sensing voltage will be presented in Section IV-D.

From Fig. 7, we can see that the number of selected response bits is related to the setting of Δf. The number increases as Δf increases. This is because less responses are able to meet with the selection criterion of $|f_i - f_j| < \Delta f$ when the Δf decreases. Notably, when the $\Delta f = 0.3$ MHz, there are still more than 15,000 response bits satisfying the selection criterion while ensuring the difference between $\hat{p}_{interPQ}$ and $\hat{p}_{intraPQ}$ is more than 35%, which significantly improves the sensing capability as will be evaluated in Table. I.

Fig. 8 shows the $\hat{p}_{intraPQ}$ and $\hat{p}_{interPQ}$ of five ROPUFs implemented in five different FPGA boards. The sensitive response selection algorithm is applicable to all five ROPUF sensors. The large difference between $\hat{p}_{intraPQ}$ and $\hat{p}_{interPQ}$ facilitates the distinguishing of V_i, where $V_i \in \{0.96\text{ V}, 1.08\text{ V}, 1.20\text{ V}, 1.32\text{ V}, 1.44\text{ V}\}$, from the rest.

In practice, an user and an adversary are assigned with different security access levels to the ROPUF. Specifically,

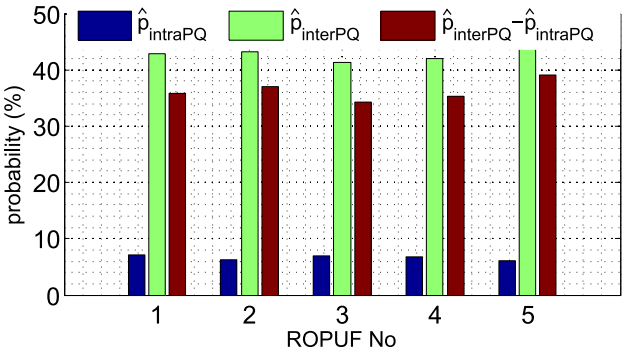

Fig. 8. The $\hat{p}_{interPQ}$ and $\hat{p}_{intraPQ}$ performance across five ROPUFs. Sensitive response bits selection is performed under the reference voltage of 1.20 V. The $\hat{p}_{intraPQ}$ is evaluated under 1.20 V as well. The Δf is set to be 0.3 MHz.

in the enrollment or provisioning phase, the user is able to obtain the RO frequency directly from the counter bypassing the comparator. This direct access is disabled/destroyed once the enrollment phase is completed [54]. The adversary needs to decompose the layer for probing if the internal RO frequency information is attempted to be measured. But this operation is more likely to change or destroy the PUF behavior.

The PUF sensor sensing based the inherent response unreliability is achieved by employing the following authenticated sensing protocol.

C. Authenticated Sensing Protocol

The authenticated sensing protocol has two phases: enrollment phase and authentication phase. It is performed as follows:

(step 1) In the *enrollment phase*, the trusted entity—user—issues a PUF sensor and measures a number of responses $\mathbf{R}_i^{PQ_j}$ for the given challenge $\mathbf{C}_i$ under different PQ_j values, e.g., different voltages, $j \in \{1, \ldots, p\}$. The user securely saves the measured CRPs in the database. Then the PUF sensor is installed in the intended (hostile) location for monitoring the PQ—e.g., voltage or other PQs that can be metered by the voltage.

(step 2) In the *authentication phase*, when collection of data from the PUF sensor is requested, the user randomly selects a challenge $\mathbf{C}$ and sends it to the PUF sensor. The PUF sensor is stimulated by the challenge $\mathbf{C}$ under PQ_i that is the voltage the PUF sensor currently working on. Consequently, the $\mathbf{R}^{PQ_i}$, $i \in \{1, ..., p\}$ is sent back to the user.

(step 3) The user compares each recorded response $\mathbf{R}^{PQ_j}$, $j \in \{1, ..., p\}$—obtained under PQ_j to the challenge $\mathbf{C}$—with the received response $\mathbf{R}^{PQ_i}$. Only the response $\mathbf{R}^{PQ_j}$, where $i = j$, stored in the database will match the received response $\mathbf{R}^{PQ_i}$ given the same queried challenge $\mathbf{C}$. If the user finds that one of the saved response $\mathbf{R}^{PQ_j}$ matches the received $\mathbf{R}^{PQ_i}$. Then the sensed value of PQ_i is discovered. Otherwise, this round of authenticated sensing is rejected.

In step 3, the success of authenticated sensing relies on the fact that the intraPQ-distance is less than the interPQ-distance

TABLE I

QUANTITATIVE EVALUATION OF NECESSARY BIT LENGTH OF THE RESPONSE FOR AUTHENTICATED SENSING UNDER DIFFERENT $\hat{p}_{\text{interPQ}}$ AND $\hat{p}_{\text{intraPQ}}$ THAT ARE DETERMINED BY Δf

			EER $< 10^{-2}$				EER $< 10^{-4}$				EER $< 10^{-6}$			
Δf MHz	$\hat{p}_{\text{intraPQ}}$	$\hat{p}_{\text{interPQ}}$	n	n_{EER}	FAR*	FRR*	n	n_{EER}	FAR*	FRR*	n	n_{EER}	FAR*	FRR*
3	1.51%	9.62%	148	7	−2.02	−2.12	372	17	−4.02	−4.16	614	28	−6.01	−6.39
2	1.91%	12.12%	116	7	−2.01	−2.15	293	17	−4.02	−4.20	472	27	−6.01	−6.15
1	3.30%	21.04%	65	7	−2.01	−2.25	158	16	−4.06	−4.11	258	26	−6.04	−6.22
0.5	5.44%	34.24%	34	6	−2.01	−2.03	89	15	−4.11	−4.05	143	24	−6.01	−6.05
0.3	7.10%	42.90%	30	7	−2.12	−2.36	68	15	−4.03	−4.16	111	24	−6.13	−6.09

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

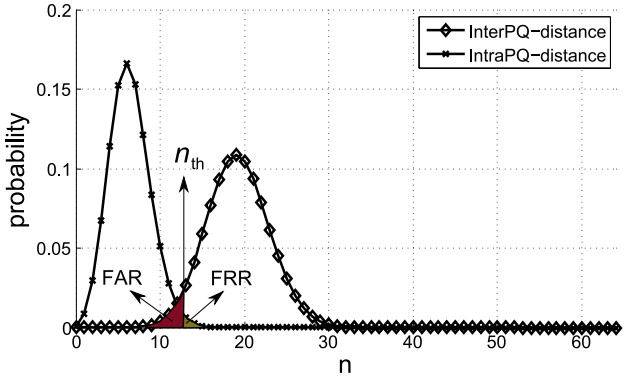

Fig. 9. Illustration of distribution of interPQ-distance and intraPQ-distance for a 64-bit response.

as illustrated in Fig. 9. For example, in Fig. 4, responses under V_1, V_2, V_3, V_4 are divergent to the same challenge referring to the interPQ-distance. In contrast, the response is relatively stable when it is reproduced under the same $V_j,\ j \in \{1, 2, 3, 4\}$ as shown by the intraPQ-distance distribution. The recorded response $\mathbf{R}^{\text{PQ}}$ matches the received response $\mathbf{R}^{\text{PQ}_j}$ only when they are generated under the same PQ_j for the same challenge queried to the same PUF sensor.

There might be a need for calibration to traditional sensors, in contrast, PUF sensors do not require calibration as the response enrolling during the enrollment phase is equivalent to the calibration operations.

D. Sensing Capability

To correctly recover a specific PQ value, one single CRP is not enough. Multiple response bits or a number of CRPs are necessary to reduce the error for both mistakenly accepting a response when it is generated under a false PQ value, referred as false acceptance rate (FAR), and falsely reject the authentic response when it is a result of a genuine PQ value, referred as false rejection rate (FRR). It is imperative to minimize both FAR and FRR in practice when a PUF sensor is employed in field to recover the PQ value based on the authenticated sensing protocol. More generally, 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.

These two undesirable errors are illustrated in Fig. 9. The right tail of the intraPQ-distance distribution indicates the FRR, while the left tail of the interPQ-distance distribution implies the FAR. When the length of response bits or the number of CRPs, n, and the threshold n_{th} used for authenticated sensing are given, and considering that both interPQ-distance and intraPQ-distance follow a binomial distribution, then the FAR and FRR can be formally expressed following work in [37] and [55]:

$$\text{FRR} = 1 - \sum_{i=0}^{n_{\text{th}}} \binom{n}{i} (\hat{p}_{\text{intraPQ}})^i (1 - \hat{p}_{\text{intraPQ}})^{(n-i)}, \quad (5)$$

$$\text{FAR} = \sum_{i=0}^{n_{\text{th}}} \binom{n}{i} (\hat{p}_{\text{interPQ}})^i (1 - \hat{p}_{\text{interPQ}})^{(n-i)}. \quad (6)$$

From the security and practicability perspectives, the FAR expresses the security of the authenticated sensing approach, because a high FAR indicates a high risk of incorrectly accepting a false PQ value, which could rise a security concern. The FRR expresses the robustness or usability of the authenticated sensing approach and indicates the probability of misrejecting an authentic PQ value.

Based on (5) and (6), we can see that the FRR and FAR depend on the $\hat{p}_{\text{intraPQ}}$ and $\hat{p}_{\text{interPQ}}$, the threshold n_{th}, and the number of employed CRPs n. For example, supposing n is 64 as shown in Fig. 9, a large n_{th} benefits the false rejection rate but aggravates the false acceptance rate, and vice versa for a small n_{th}. We want to balance them in practice. There exists a threshold value to make both FAR and FRR equal. We refer this interested threshold value as *equal error threshold*, termed n_{EER}. Consequentially, when both error rates are equal, we refer this equal rate as *equal error rate* (EER) following Roel's work [37]. 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 [37]:

$$n_{\text{EER}} = \underset{n_{\text{th}}}{\text{argmin}}\{\max\{\text{FAR}(n_{\text{th}}), \text{FRR}(n_{\text{th}})\}\}, \quad (7)$$

$$\text{EER} = \max\{\text{FAR}(n_{\text{EER}}), \text{FRR}(n_{\text{EER}})\}. \quad (8)$$

Given PUF sensors with binomial probability estimator $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$, the task is to find minimal number of CRPs, n, for ensuring an acceptable EER that meet desired requirements, e.g., a value lower than 10^{-6}.

TABLE II
PUF SENSOR RESOLUTION SUMMARY

PQ	resolution	PUF kernel
Temperature	4°C	XOR4 BR-PUF [14]
Distance	100 um	Optical PUF [14]
Voltage	0.12 V	ROPUF (our work)

In Table. I, we give quantitative evaluations of n—minimal bit length of the response to meet the EER, and n_{th} of PUF sensors under different $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$. Reader is reminded that both $\hat{p}_{\text{interPQ}}$ and $\hat{p}_{\text{intraPQ}}$ are influenced by the chosen Δf as shown in Fig. 6. The used PQ in this table is voltage. We can see from Table. I, necessary bit length of n decreases as Δf is reduced. This indicates the efficiency of the authenticated sensing approach and the need to implement the proposed sensitive response bits selection method. For example, n is reduced by more than 80% by shrinking Δf from 3 MHz to 0.3 MHz when both FAR and FRR are guaranteed to be less than 10^{-6}. Using selected sensitive bits that are more sensitive for discovering sensed PQ value expedite protocol as less response bits need to be acquired on the PUF sensor during operation. In addition, the volume needed to securely store responses in database is reduced or relaxed.

We summarize the PUF sensor resolution to various PQs reported from *experimental* results in Table II. As the work from [14] does not evaluate the sensing capability and consider sensitive response selection, we do not compare the necessary number of responses to achieve a given sensing capability with them. The ROPUF sensor gives 0.12 V resolution. Notably, this experimentally validated resolution is limited by the available voltage interval—only five voltage settings, 0.96 V, 1.08 V, 1.20 V, 1.32 V and 1.44 V, are evaluated and available. In addition, better voltage resolution can be achieved by employing more sensitive responses. Here, using the universal voltage ROPUF sensor, we assess humidity and temperature resolution using a voltage-out humidity and temperature sensor (HHT2M1HH2M1, Hanwei). Its operating range is 0-100% RH for humidity and 0-80°C for temperature. The relationship between relative humidity and voltage is 33.3%RH/1V. The relationship between temperature and voltage is 1°C/0.01V. Therefore, the ROPUF sensor can achieve a relative humidity resolution of 4% RH and a temperature resolution of 12 °C.

In some applications, feeding the sensed signal directly to power rail of the ROPUF can result in dynamic range measurement limitation. A potential approach to address this limitation is to convert the corresponding sensed parameter to current that can be used to control the reference current passing through the RO, hence improving the dynamic range.

V. DISCUSSION

Physical attacks on some PUFs are feasible, they are, however, usually more complicated in comparison with physical attacks on the digital secrets stored in the NVM as keys in the traditional crypto module. Notably, physical attacks on PUFs are always requiring power-on of the supply voltage, because the secrets are only presented on demand rather than preserved all the time as the digital secrets in the NVM. Moreover, invasive physical attacks such as delayering chips of the PUFs are more likely to alter or even destroy the PUF secrets once the PUF circuit layout is carefully considered [4], [36].

It is noticed that the localized electromagnetic (EM) attack is feasible in case of ROPUFs [56], [57], while it requires certain professional skills and accurate calibration equipments to scan the entire die surface according to the X-Y coordinate. There are several countermeasures. Firstly, the path between the RO and the multiplexer and subsequent counter can be randomized and configured by the challenge vector to decorrelate the relation between the RO and the measurement path. The second countermeasure is more efficient, which employs interleaved placement. In this context, there is no extra area and power cost by interleaving ROs and other components such as multiplexers, comparators and counters using careful placement and routing techniques.

In the following, we focus on countermeasures of replaying and man-in-the-middle attacks by adopting the reverse/reusable fuzzy extractor [48], [58] allowing multiple usage of the same challenge. Then we discuss mitigation of influence from the unwanted PQ, e.g., temperature.

A. Reverse Fuzzy Extractor

In the authenticated sensing protocol, CRPs are exposed directly without protection and communicated between the PUF sensor and the user. An adversary may eavesdrop on the CRPs and therefore exploit them for replaying attacks.

To avoid replaying attacks, each CRP is only used once. Such an attack is avoided naturally, if a strong PUF is available—this is because it generates a large number of CRPs that cannot be fully characterized within a short time (e.g. less than a few months). Unfortunately, a cost-effective and compact strong PUF may not be always available, especially, considering modeling attacks [12], [59]. Weak PUFs such as SRAM PUFs and ROPUFs [26], [27], [52] are more commonly used. For example, SRAM PUFs are free of the requirement for custom design. The ROPUF has an advantage of unrestricted layout during design phase. In this context, the fuzzy extractor can be employed to post-processing the response, while still able to prevent replaying attacks and man-in-the-middle manipulation in insecure communication channels.

In PUF-based key generation applications, the *fuzzy extractor* is employed [60]. The fuzzy extractor consists of two parts: *secure sketch* and *randomness extractor*. Secure sketch eliminates noise from the collected noisy data. In other words, it maps the similar regenerated response into the same value. Randomness extractor guarantees the uniform distribution/randomness of derived keys based on the corrected response.

There are two steps involved in the secure sketch. The first step is to generate the *helper data* that is computed from the PUF response $\mathbf{R}$ during helper data generation phase. In the second step, the helper data is employed to recover the original response $\mathbf{R}$ from the afterward regenerated response $\mathbf{R}'$, where

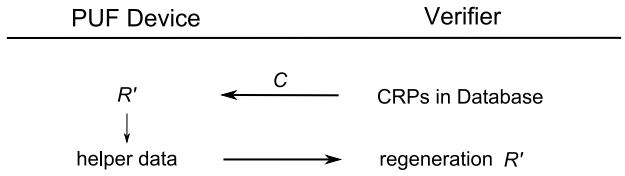

Fig. 10. Reverse fuzzy extractor [58].

the difference between the original response $\mathbf{R}$ and reproduced response $\mathbf{R}'$ is small. Usually, the helper data generation is performed at the user/verifier side, while the reconstruction of the original $\mathbf{R}$ is implemented in the PUF integrated device.

Note that implementing a decoding logic in the PUF integrated device to recover the original $\mathbf{R}$ results in higher area and power overhead, reverse or reusable fuzzy extractor is proposed [48], [58] to overcome this issue. Fig. 10 illustrates the simplified structure of the reverse fuzzy extractor. The reverse fuzzy extractor moves the computation heavy decoding operation to the resource-rich verifier, while leaving the lightweight helper data generation to the PUF integrated device. It can be seen that the PUF integrated device generates new helper data based on the reproduced response $\mathbf{R}'$ whenever the authenticating of the PUF device is requested. The verifier carries out the computationally intensive decoding to recover the reproduced response $\mathbf{R}'$ based on the recorded response $\mathbf{R}$ and the helper data from the PUF device, then performs the authentication.

The reverse fuzzy extractor enables multiple usage of the same CRP when preventing replaying attacks, and it is also secure despite the possibility of physical access to the PUF and the eavesdropping occurrence. This is because the regenerated response $\mathbf{R}'$ is invisible to the adversary—only helper data is observable. In addition, each regeneration of response $\mathbf{R}'$ gives rise to a new helper data. Even multiple executions of helper data generation leak some information, the reverse fuzzy extractor based on the syndrome construction [48], [61] is able to ensure a min-entropy in the PUF response.

Therefore, the lightweight reverse fuzzy extractor can be employed to counteract possible attacks such as replaying attacks as well as man-in-the-middle manipulations through the insecure communication channel as an alternative to employ a strong PUF if it is not available. Moreover, the reverse fuzzy extractor does not need PUFs to have a large CRP space. Therefore, PUFs limited by the number of CRPs, e.g., SRAM PUF, typical ROPUF [6], can also be securely deployed as a kernel for the PUF sensor.

B. Mitigating the Influence From the Unwanted PQ

As stated in the definition of PUF sensor in Section II-B, the response bit of a PUF sensor should be stable when the uninterested PQ varies. In our study, the PQ of interest is voltage, while the reliability degradation originating from temperature variations is unwanted. In other words, the response bit is preferred to be stable within a wide range of temperature variations.

This concern can be addressed by harnessing the negative temperature coefficient of current starved inverters to compensate the positive temperature coefficient of regular inverters in order to prevent response bits flipping due to temperature fluctuations [62]. The current starved inverters and regular inverters can be combined to construct a RO. Such circuits can be designed to ensure the coefficient between the temperature and the frequency of the RO is invariant to the temperature fluctuations. Based on the experimental data given in [62], the reliability of ROPUF is nearly 100% when the temperature changes from -20°C to 120°C—the reference temperature is 27°C and the voltage is fixed at 1.2 V.

VI. Conclusion

This work takes advantage of unreliable response bits of conventional PUFs to lend themselves as universal PUF sensors, because those unreliable responses are sensitive to environmental parameters, specifically, the voltage. We formalize the properties of a PUF sensor and present an authenticated sensing protocol applicable to the PUF sensor. This protocol impedes sensory data spoofing without reliance on traditional cryptographic algorithms and trusted communication channels. In addition, we proposed a method of selecting unreliable response bits to expedite the enrollment phase and also greatly cutting down the necessary bit length of the response during authenticated sensing phase. The quantitative analyses of bit length of response to perform the sensing protocol are based on experimental data. The practicability and security analyses validate the PUF sensor as a lightweight alternative for secure wireless sensing, especially when the sensed PQ has higher security concern while the resolution requirement is not that strict, for examples, to securely sense: hot, warm, cold; or too bright, normal bright, dark. If the PUF sensor is used to extract cryptographic keys, it enables more interesting applications [2]. For example, encoding a message in such a way that the message can only be decrypted under a specific PQ range, e.g., under dark or under a quiet sound background.

We, however, do realize several challenges in designing a more efficient PUF sensor [2], [14], [16]. Firstly, to increase the resolution of sensing, the sensitivity of response generation's reliance on the PQ needs to be amplified besides utilizing more number of sensitive response bits. Secondly, storage of large number of CRPs currently necessary for our authenticated sensing protocol should ideally be avoided to ease the management and scalability of the PUF sensor usage. This could be achieved by storing a parameter model of the PUF sensor and later emulating necessary CRPs as in [9] and [54]. Thirdly, selection of interested unreliable response bits that are sensitive to a specific PQ needs an improved approach and ideally one that is applicable to other popular PUF constructions, such as APUFs while maintaining its security. Our future work will investigate these challenges.

Acknowledgment

The authors would like to thank Dr. Damith C. Ranasinghe and anonymous reviewers for their reviews and suggestions to improve the quality of the paper.

REFERENCES

[1] T. Abera *et al.*, "Invited-things, trouble, trust: On building trust in IoT systems," in *Proc. 53rd Annu. Design Autom. Conf.*, 2016, p. 121.

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

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

[4] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, 2002, pp. 148–160.

[5] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurrency Comput. Pract. Exper.*, vol. 16, no. 11, pp. 1077–1098, 2004.

[6] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Design Autom. Conf.*, 2007, pp. 9–14.

[7] 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, Mar. 2016.

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

[9] Y. Gao *et al.*, "Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2016, pp. 1–6, doi: 10.1109/PERCOMW.2016.7457162.

[10] D. Lim, "Extracting secret keys from integrated circuits," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2004.

[11] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 237–249.

[12] U. Rührmair *et al.*, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov. 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*. Berlin, Germany: Springer, 2015, pp. 535–555.

[14] U. Rührmair *et al.*, "Virtual proofs of reality and their physical implementation," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 70–85.

[15] Y. Cao, L. Zhang, S. S. Zalivaka, C.-H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for coherent sensor-level authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 11, pp. 2629–2640, Nov. 2015.

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

[17] H. Ma, Y. Gao, O. Kavehei, and D. C. Ranasinghe, "A PUF sensor: Securing physical measurements," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, 2017.

[18] U. Rührmair, "On the formal foundations of PUFs and related primitives," Ph.D. dissertation, Faculty IV—Elect. Eng. Comput. Sci., Tech. Univ. Berlin, Berlin, Germany, 2016.

[19] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[20] P. S. Ravikanth, "Physical one-way functions," Ph.D. dissertation, School Archit. Planning, Massachusetts Inst. Technol., Cambridge, MA, USA, 2001.

[21] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[22] S. S. Zalivaka, A. V. Puchkov, V. P. Klybik, A. A. Ivaniuk, and C.-H. Chang, "Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation," in *Proc. 21st Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2016, pp. 533–538.

[23] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, 2011.

[24] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2014, pp. 1–6, doi: 10.1145/2593069.2593072.

[25] J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon PUFs and recent advances in ring oscillator PUFs," *J. Comput. Sci. Technol.*, vol. 29, no. 4, pp. 664–678, 2014.

[26] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sep. 2009.

[27] S. Zeitouni, Y. Oren, C. Wachsmann, P. Koeberl, and A.-R. Sadeghi, "Remanence decay side-channel: The PUF case," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1106–1116, Jun. 2015.

[28] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE J. Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan. 2008.

[29] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," in *Proc. 3rd Benelux Workshop Inf. Syst. Secur. (WISSec)*, 2008, pp. 1–17.

[30] V. van der Leest, G.-J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware intrinsic security from D flip-flops," in *Proc. 5th ACM Workshop Scalable Trusted Comput.*, 2010, pp. 53–62.

[31] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 67–70.

[32] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, "A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1137–1150, Jun. 2015.

[33] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based PUF," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 2071–2074.

[34] R. Kumar and W. Burleson, "On design of a highly secure PUF based on non-linear current mirrors," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 38–43.

[35] A. Herkle, J. Becker, and M. Ortmanns, "Exploiting weak PUFs from data converter nonlinearity—E.g., a multibit CT $\Delta\Sigma$ modulator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 7, pp. 994–1004, Jul. 2016.

[36] M. Wan, Z. He, S. Han, K. Dai, and X. Zou, "An invasive-attack-resistant PUF based on switched-capacitor circuit," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 8, pp. 2024–2034, Aug. 2015.

[37] M. Roel, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, Dept. Elect. Eng., Katholieke Univ. Leuven, Leuven, Belgium, 2012.

[38] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[39] L. Zhang, Z. H. Kong, C.-H. Chang, A. Cabrini, and G. Torelli, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 921–932, Jun. 2014.

[40] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "mrPUF: A novel memristive device based physical unclonable function," in *Applied Cryptography and Network Security*. Cham, Switzerland: Springer, 2015, pp. 595–615.

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

[42] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable spin-transfer torque magnetic RAM-based physical unclonable function with multi-response-bits per cell," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1630–1642, Aug. 2015.

[43] J. Rajendran *et al.*, "Nano meets security: Exploring nanoelectronic devices for security applications," *Proc. IEEE*, vol. 103, no. 5, pp. 829–849, May 2015.

[44] 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.

[45] U. Rührmair *et al.*, "Method for security purposes," U.S. Patent Appl. 13/250 534, Sep. 30, 2011.

[46] B. Fisch, D. Freund, and M. Naor, "Physical zero-knowledge proofs of physical properties," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2014, pp. 313–336.

[47] X. Xu, U. Rührmair, D. E. Holcomb, and W. Burleson, "Security evaluation and enhancement of bistable ring PUFs," in *Proc. Int. Workshop Radio Freq. Identificat., Secur. Privacy Issues*, 2015, pp. 3–16.

[48] R. Canetti, B. Fuller, O. Paneth, L. Reyzin, and A. Smith, "Reusable fuzzy extractors for low-entropy distributions," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2016, pp. 117–146.

[49] K. Kursawe, A.-R. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls, "Reconfigurable Physical Unclonable Functions—Enabling technology for tamper-resistant storage," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jul. 2009, pp. 22–29.

[50] S. Katzenbeisser, Ü. Kocabaş, V. van der Leest, A.-R. Sadeghi, G.-J. Schrijen, and C. Wachsmann, "Recyclable PUFs: Logically reconfigurable PUFs," *J. Cryptograph. Eng.*, vol. 1, no. 3, pp. 177–186, 2011.
[51] S. S. Mansouri and E. Dubrova, "Ring oscillator physical unclonable function with multi level supply voltages," in *Proc. 30th Int. Conf. Comput. Design*, Sep. 2012, pp. 520–521.
[52] D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proc. Conf. RFID Secur.*, 2007, pp. 1–12.
[53] A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 94–99.
[54] 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 Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 3, pp. 146–159, Jul./Sep. 2016, doi: 10.1109/TMSCS.2016.2553027.
[55] 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, Oct. 2005.
[56] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, "Semi-invasive EM attack on FPGA RO PUFs and countermeasures," in *Proc. Workshop Embedded Syst. Secur.*, 2011, p. 2.
[57] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of RO PUFs," in *Proc. Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2013, pp. 19–24.
[58] A. Van Herrewege *et al.*, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," in *Financial Cryptography Data Security*. Berlin, Germany: Springer, 2012, pp. 374–389.
[59] G. T. Becker, "On the pitfalls of using Arbiter-PUFs as building blocks," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 34, no. 8, pp. 1295–1307, Aug. 2015.
[60] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2004, pp. 523–540.
[61] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, 2004, pp. 82–91.
[62] 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 Des. Integr. Circuits Syst.*, vol. 34, no. 7, pp. 1143–1147, Jul. 2015.

Yansong Gao (S'15) received the B.Sc. degree in electronic information science and technology from the Henan University of Science and Technology, Luoyang, China, in 2008, and the M.Sc. degree in signal information processing from the University of Electronic Science and Technology of China, Chengdu, China, in 2013. He is currently pursuing the Ph.D. degree with the School of Electrical and Electronic Engineering, The University of Adelaide.

His current research interests are hardware security circuit designs and their applications, mainly focus on physical unclonable functions, machine learning, and memristive device characterization.

Hua Ma received the B.Sc. degree in electronic information science and technology from the Henan University of Science and Technology, Luoyang, China, in 2008. She is currently a Research Assistant with the Adelaide Auto-ID Labs, School of Computer Science, The University of Adelaide. Her research interests are physical unclonable function related applications, and circuit design.

Derek Abbott (M'85–SM'99–F'05) was born in London, U.K., in 1960. He received the B.Sc. degree (Hons.) in physics from Loughborough University, Leicestershire, U.K., in 1982, and the Ph.D. degree in electrical and electronic engineering from The University of Adelaide, Adelaide, SA, Australia, in 1995, under the supervision of K. Eshraghian and B. R. Davis.

From 1978 to 1986, he was a Research Engineer with the GEC Hirst Research Centre, London, U.K. From 1986 to 1987, he was a VLSI Design Engineer with Austek Microsystems, Australia. Since 1987, he has been with The University of Adelaide, where he is currently a Full Professor with the School of Electrical and Electronic Engineering. He co-edited the book *Quantum Aspects of Life* (London, U.K.: Imperial College Press, 2008), co-authored *Stochastic Resonance* (Cambridge, U.K.: Cambridge University Press, 2012), and co-authored *Terahertz Imaging for Biomedical Applications* (New York, NY, USA: Springer-Verlag, 2012). He holds over 800 publications/patents and has been an invited speaker at over 100 institutions. His interests are in the area of multidisciplinary physics and electronic engineering applied to complex systems. His research programs span a number of areas of stochastics, game theory, photonics, biomedical engineering, and computational neuroscience.

Prof. Abbott is a fellow of the Institute of Physics. He has won a number of awards, including the South Australian Tall Poppy Award for Science (2004), the Premier's SA Great Award in Science and Technology for outstanding contributions to South Australia (2004), an Australian Research Council Future Fellowship (2012), and the David Dewhurst Medal (2015). He has served as an Editor and/or Guest Editor for a number of journals, including the IEEE JOURNAL OF SOLID-STATE CIRCUITS, the *Journal of Optics B*, the *Microelectronics Journal*, *Chaos*, *Smart Structures and Materials*, *Fluctuation and Noise Letters*, the PROCEEDINGS OF THE IEEE, the IEEE PHOTONICS JOURNAL, and *Plosone*. He is currently on the editorial boards of the Nature's Scientific Reports, the IEEE Access, the Royal Society Open Science, and the Frontiers in Physics.

Said F. Al-Sarawi (S'92–M'96) received the General Certificate in marine radio communication and the B.Eng. degree (Hons.) in marine electronics and communication from Arab Academy for Science and Technology, Alexandria, Egypt, in 1987 and 1990, respectively, and the Ph.D. degree in mixed analog and digital circuit design techniques for smart wireless systems with special commendation in electrical and electronic engineering and the Graduate Certificate in education (higher education) from The University of Adelaide, Adelaide, SA, Australia, in 2003 and 2006, respectively.

He is currently the Director of the Centre for Biomedical Engineering and a Founding Member of the Education Research Group of Adelaide (ERGA), The University of Adelaide. His current research interests include design techniques for mixed signal systems in complementary metal–oxide–semiconductor and optoelectronic technologies for high-performance radio transceivers, low-power and low-voltage radio-frequency identification systems, data converters, mixed signal design, and microelectromechanical systems for biomedical applications. His current educational research is focused on innovative teaching techniques for engineering education, research skill development, and factors affecting students evaluations of courses in different disciplines.

Dr. Al-Sarawi was a recipient of The University of Adelaide Alumni Postgraduate Medal (formerly Culross Prize) for outstanding academic merit at the post-graduate level. While pursuing the Ph.D., he won the Commonwealth Postgraduate Research Award (Industry).