# Exploiting Unreliability of the PUF to Secure Remote Wireless Sensing

Yansong Gao[1,2], Hua Ma[2], Damith C. Ranasinghe[2], Said F. Al-Sarawi[1], and Derek Abbott[1]

[1] School of Electrical and Electronic Engineering,
The University of Adelaide, SA 5005, Australia,
{yansong.gao, said.alsarawi, derek.abbott}@adelaide.edu.au,
[2] Auto-ID Labs, School of Computer Science,
The University of Adelaide, SA 5005, Australia,
{mary.ma, damith.ranasinghe}@adelaide.edu.au

**Abstract.** Wireless sensors attracts increasingly attention from both academia and industry owing to emerging applications built upon them such as Internet of Things, smart home, E-Health, and etc. It becomes a concern that the sensed value should be trusted in such applications scenarios. The security of the sensor used to resort to traditional cryptographic techniques, which, however, only provides limited protection by virtue of its vulnerability to physical attacks and may not economically viable. In this paper, we propose a new sensing methodology making remote sensing highly secure. In particular, we facilitate the susceptibility of physical unclonable function (PUF) to ambient environment variations, acting as a PUF sensor, to grantee the veracity of the sensing value even the PUF sensor is located in an untrusted remote location and the communication channel is also insecure without implementing relatively expensive crypto module. The PUF sensor is cost-efficient and most importantly anti-counterfeiting, while offers high level security. We demonstrate the practicability of the PUF sensor based on experimental implementations. In addition, we show that the extended sensing functionality of a PUF is actually improving PUF's resistance against modeling attacks.

**Keywords:** remote sensing, hardware security, physical unclonable function, modeling attacks.

## 1 Introduction

Wireless sensors are widely used in our daily lives such as monitoring wildfires, traffic, building security, or patient's movement. There are emerging applications such as building smart home, smart city, and Internet of Things that depends on the remote installed sensors. Genuineness of the measurement of the sensor forms a security foundation in aforementioned applications. If the measurement sent to the user is spoofed, it may lead to incorrect decisions, and consequently may threat personal safety. The security of the sensor, traditionally, relies on the separated crypto modules encrypting measurement from analog sensors. This standalone cryptographic solution, usually, is hindered in practice as a fact that most wireless sensors having very limited room to implement a relatively pricey separately crypto module. Moreover, cryptographic algorithm executed in the crypto module suffers physical attacks.

The emerging hardware security primitive—physical unclonable function (PUF)—provides a promising lightweight security solution for lightweight devices [1, 2]. A PUF is a tiny hardware device exploiting uncontrollable process variations to extract unique signatures inherent to the device itself, which cannot be cloned and inherently resistant to tamper attacks or side channel attacks [3, 4]. A PUF results in a response (response) determined by the complexed physical function and the input (challenge). The physical function is derived from the inherent static randomness originated from unavoidable fabrication process. Therefore, responses produced from different PUF instances with the same design are different for a given challenge. The PUF is expected to regenerate the same response when it is stimulated by the same challenge. However, in practice, it is susceptible to ambient environment changes. In typical PUF-oriented applications, eg. cryptographic key generation [5], it is favorable to reduce the unreliability to ease the error correction on the unreliable responses. Even in PUF-based authentication applications [2] showing some degree tolerance to unreliability, it is still important to minimize it as low as possible since it ease the complexity of modeling attacks [6–8].

In contrast, we utilize this unavoidable unreliability of a PUF to provide high degree of assurance of measured data, where the PUF itself is a sensor considering that the regeneration of a response is sensitive to a environmental parameter, eg. voltage or temperature. Considering the unreliable response shows distinct values when the temperature or voltage deviates. The unreliable response under a specific

temperature or voltage becomes reliable when it is regenerated under a different temperature or voltage. Different responses will be regenerated under different environmental parameter for the same challenge stimulated the same PUF. As a consequence, unreliable responses—reversely—reflect the change of the environmental parameter. In such cases, the PUF itself is treated as a sensor as a result of the unreliable response sensitive to the environmental changes.

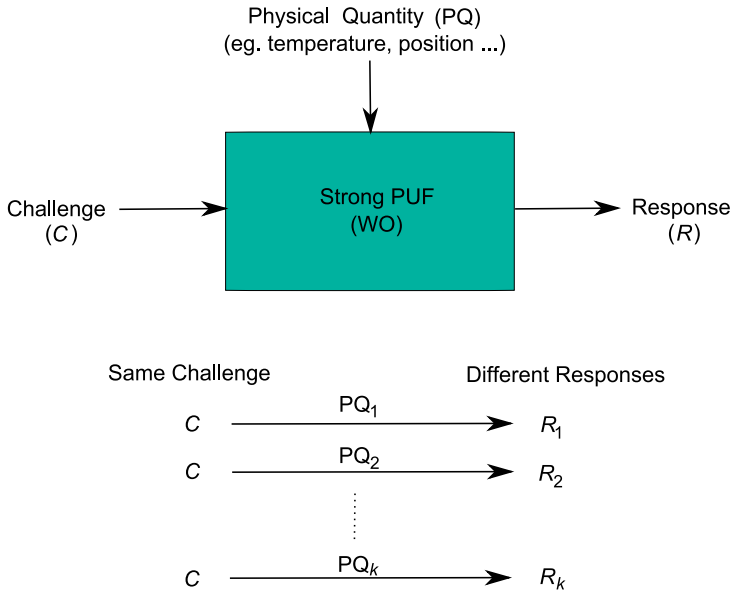


**Fig. 1.** PUF as a sensor. The response is determined by both the PQ and the given challenge.

Using the PUF as a sensor to measure a particular physical quantity (PQ)—an environmental parameter— has been proposed by Rosenfeld *et al.* [9]. The authors conceived merging sensing with cryptography by making most of the PUF to avoid separated crypto module and traditional sensor architecture that is may vulnerable to attacks. Note in [9], the optical coating based PUF is not exmperitally fabricated. Its performance is evaluated through simulation to demonstrate the feasibility of sensing the PQ—light. Further, it is specifically designed to take both a PQ—specifically light in [9]—and challenge as input of the PUF, as a consequence, the response is not only determined by the challenge itself but also the PQ of light, see figure 1. Ruhrmair *et al.* [10] experimentally demonstrate the responses is also a function of temperature to proof the new security concept, virtual proof of reality—a complementary security concept to physical zero-knowledge protocols [11]—that enables the proof of a physical statement over an untrusted digital communication channel between two parties (a prover and a verifier). However, it is observed the response dependence on the temperature is not enough strong leading to greatly length increasing of the response to successfully sensing temperatures that the PUF works in.

In this paper, we distinguish our work from the previous works. i) In comparison with [9], firstly, we use experimental data rather through simulation. Secondly, The PUF requires no specific materials such as optical coating in [9], which costs no extra fabrication process. We exploit the unreliable responses—generally, an undesirable performance of a PUF—for secure remote sensing applications. ii) In comparison with [10], firstly, the length of the response significantly decreased thanks to the method we proposed to select unreliable response bits that are highly dependent on the voltage. Secondly, we demonstrate the voltage can be effectively sensed, where in [10], the feasibility of sensing temperature and position is demonstrated. Our contributions in this paper are:

1. We extend the conventional PUF to be a sensor by exploiting its unreliability to secure wireless remote sensing measurements—in particular, the voltage—without implementing a separate crypto module. While the extended sensing function has no influence on the PUF's performance when it still serves as an trust anchor bounded to a device.
2. We experimentally demonstrate the practicability of our proposed wireless sensing methodology using PUF sensor through experimental data collected from five ring oscillator PUFs (ROPUFs) [2, 12, 13] implemented in five FPGA boards.

3. We present an approach to fasten the selection of unreliable responses that are strongly dependent on the voltage to decrease the length of the response for sensing.
4. We show that the unreliability of PUF can increase resistance to modeling attacks that is a powerful attack to break a PUF.

The rest of the paper organized as follows. Related works including PUF and the definition of PUF sensor are introduced in Section 2. Section 3 illustrate the feasibility of exploiting the unreliability of the PUF to secure remote voltage sensing. Then experimental validation is carried out in Section 4. It also demonstrates the sensing functionality of a PUF can help to increase PUF's resistance to modeling attacks. Section 5 concludes the paper.

## 2 Related Work

### 2.1 Physical Unclonable Functions

Pappu *et al.* introduced an optical PUF in 2001 [**?**,14], also called a physical one-way function, where the response (speckle pattern) is dependent on the input laser location/polarization (i.e. challenge) when the laser irradiates a stationary scattering medium. The Optical PUF, however, requires large and expensive external measurement devices. Moreover, its reliability is highly dependent on very accurate calibration of the input location. Furthermore, it is difficult to integrate the Optical PUF into a resource-constraint hardware device such a contactless smart card.

Following this prototype PUF, a practical implementation of a microelectronic circuit based PUF initially called a Physical Random Function, later termed the Arbiter PUF (APUF), was proposed by Gassend *et al.* [15]. The APUF 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 individual stages where the path through each stage is determined by a corresponding bit in a challenge (i.e input bit vector). This structure is simple and capable of generating an exponential number of CRPs. However, an APUF is based on linear additive blocks and is demonstrated to be vulnerable to model building attacks [6, 16, 17] if an adversary is able to gain access to CRPs either by eavesdropping or through directly measuring the PUF to collect CRPs. To increase the complexity of such model building attacks, more variants of APUFs were proposed such as the XOR-APUF [2, 6] and the feed forward APUF [6, 1]. Another issue that results from the APUF architecture is the inconsistent responses to repeated application of certain challenges due to the arbitrator—a latch that determines the winning signal path—entering into a metastable state. To circumvent the metastability leading to aggravated reliability in APUFs and the inconvenience of implementing APUFs in an FPGA platform, another time delay based PUF, RO PUF (Ring Oscillator PUF), is first proposed in [2] and further improved [18–20]. An overview of different RO PUFs can be found in [21].

A typical RO-PUF circuit consists of $k$ ring-oscillators, two $k$-to-1 multiplexers that select a pair of ring-oscillators, $\mathrm{RO}_i$ and $\mathrm{RO}_j$, two counters and a comparator, as shown in Fig. 2. All the ring-oscillators in this structure are identical. Ideally, the frequency of each oscillator is unique, however, because the oscillating frequency is a function of the physical device parameters, which are subject to device process variation, the oscillation frequencies of each oscillator are not all identical. Therefore, the oscillation frequencies of each pair is compared by counting this frequency using a digital counter. If $f_i < f_j$ (where $f_i$ and $f_j$ are the oscillating frequencies of $\mathrm{RO}_i$ and $\mathrm{RO}_j$, respectively) the digital comparator output will be '0', otherwise '1'. The pairing of oscillators is controlled using two digital multiplexers, each use a subset of the input challenge bits to select an oscillator.

Besides the aforementioned delay-based PUFs, there are mismatch based silicon PUFs such as the SRAM PUF [22, 23], latch PUF [24], flip-flop PUF [25, 26], butterfly PUF [27], and analog PUFs based on silicon such as the current-based PUF [28] and nonlinear current mirror based PUF [29], which exploit nonlinear dynamic characterizations of current or voltage. Comprehensive reviews of conventional PUF architectures can be found in [30, 31]. In recent years, emerging PUFs with nanotechnology are initially investigated aiming to build PUFs beyond the aforementioned conventional silicon PUFs by taking advantage of prevalent process variations as a consequence of scaling down to the nano region, and other unique properties offered in emerging nanoelectronics devices [32–35]. A review of such nano PUFs can be found in [36].

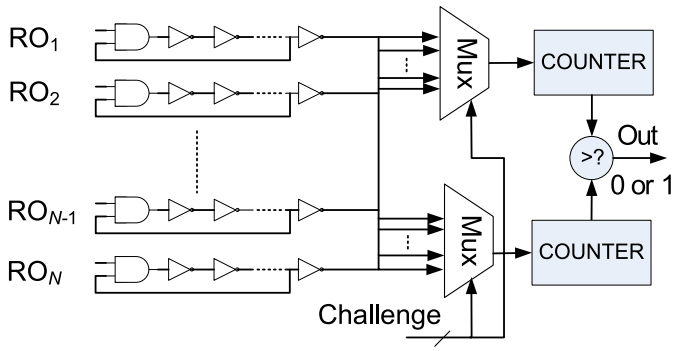


**Fig. 2.** A typical ring-oscillator PUF (RO-PUF).

### 2.2 PUF Sensor

The definition of PUF sensor is first given in [9]. A PUF sensor has the following features:

1. Its response is not only a physical function of the challenge but also strongly relies on a particular PQ.
2. Two identical PUFs cannot be manufactured.
3. The response stays relatively stable given the same challenge and the same sensed quantity.
4. Given one challenge-response pair (CRP) under a sensed quantity, no information of the response for the same challenge to a different sensed quantity can be learned.

It is practical that a PUF can satisfy such features. The inherent unreliability of PUF fits the 1) feature. The inherent randomness in manufacturing process promises the 2) and 4) features thanks the unpredictability of the responses. As the randomness is static, most responses are relatively stable. Even considering unreliable responses under a specific sensed quantity $\mathrm{PQ}_i$, they become relatively stable under the other sensed quantity $\mathrm{PQ}_j$, where $i \neq j$.

## 3 Secure Remote Sensing Based On Unreliability of The PUF

### 3.1 Reliable Responses Based on Unreliable Responses

The reliability of a PUF is the probability of regeneration of the same responses for the same challenge applied to the same PUF [37]. In practice, it is always evaluated by its complementary performance metrics—bit error rate (BER). For the same challenge applied to the same PUF, BER is the intra fractional hamming distance (intra-FHD) between the response $\mathbf{R}$ ($n$ bits) and the later regenerated response $\mathbf{R}'$. The BER is an overall assessment to all of responses generated by a PUF.

Considering the reliability of a specific 1-bit response $r$ for a given challenge. In practice, the reliability for different responses $r$, is different. In other words, it is inappropriate to evaluate the reliablity of a specific $r$ using intra-FHD. For example, for $r_1$, if the probability of generating '1's is 99% given $t$ times regenerations—there is only 1% probability for $r_1$ flipped to its unstable state, then the reliability for this specific response $r$ is 99%. It is clear that for most 1-bit responses $r$s, the reliability is 100%. While for some 1-bit responses, their reliabilities are low. If it is 50%, then it is a metastable response.

Notably, the unreliable response $r$ generated under a specific physical quantity $\mathrm{PQ}_i$ will become stable under another physical quantity $\mathrm{PQ}_j$. It is illustrated in Fig. 3. The frequency of the RO has linear relationship with the voltage applied to it. However, the linear coefficient is different from one RO to the other RO. For example, the coefficient of $\mathrm{RO}_1$ is higher than the coefficient of $\mathrm{RO}_3$ as the frequency $\mathrm{RO}_1$ oscillates faster than $\mathrm{RO}_3$ as the voltage raises. When the response regenerated under the voltage between $V_2$ and $V_3$ located at the crosspoint of $f_2$ and $f_3$. The $r_3$ will be greatly unstable because the response is strongly impacted by the noise now. However, if the voltage shifts to other point, the regeneration of $r_3$ becomes stable. For example, when $r_3$ is regenerated under the voltage $V_1$, it stably results in '1'. Where it will stably result in '0' when it is regenerated under the voltage of $V_4$.

Therefore, taking voltage into consideration when the response $r$ is regenerated given the same challenge, unreliable responses will turn to reliable responses. In Fig. 3, the large frequency difference between two ROs ensures a reliable response. The crosspoint of two frequencies always induce unstable responses. Unreliable responses becomes reliable when the voltage greatly deviates from the crosspoint.

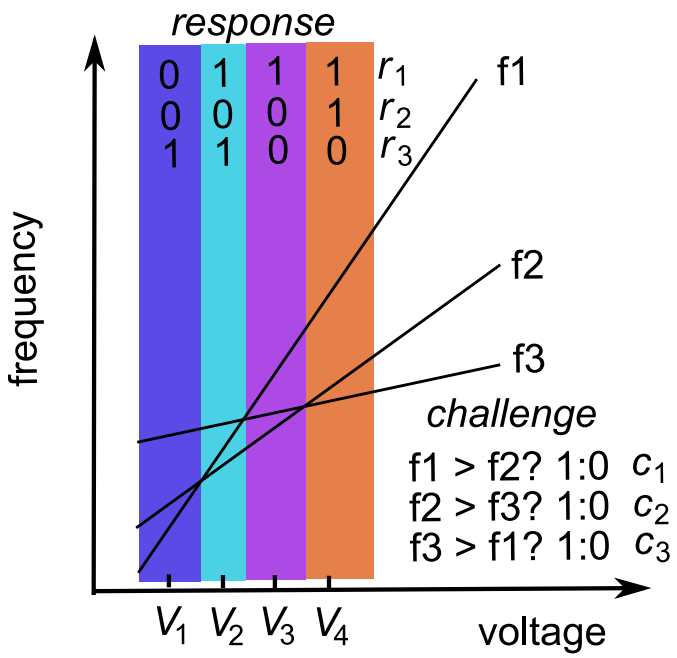


**Fig. 3.** Response is not only dependent on the challenge, it is also a function of the voltage, especially for these unreliable responses in a ROPUF.

### 3.2 Sensing Voltage Through Unreliable Responses

For some responses, they strongly depend on the voltage for the same challenge. Reversely, these responses can be exploited to discover the voltage applied to the PUF. For example, in Fig. 3, if the response **R** for the given challenge **C** is '001', then the voltage is derived as $V_1$. Similar, if it is '101', the voltage of $V_2$ is derived.

It is clear employing such a sensing approach, the response sent from the PUF sensor contains no exact voltage value. While the user can still discover the value by observe the response. This sensing scheme is secure due to an adversary cannot spoof the user with the faked voltage value, because there is no such value communicated between the sensor and the user. Further, the adversary cannot send faked counterfeit response to the user due to the response for a given challenge is unpredictable. If the adversary does send a guessed response to the user, the user is able to reject the fraudulent response.

The sensing based on the unreliability of the PUF is realized with the help of the following authentication sensing protocol.

### 3.3 Authentication Sensing Protocol

The authentication sensing protocol is performed as follows:

1. In enrollment phase, the user prepares a PUF and measures a number of responses $\mathbf{R_i}^{\mathrm{PQ_j}}$ for the given $C_i$s under different $\mathrm{PQ}_j$s—eg. different voltages. The user saves the measured CRPs in the database. Then the PUF sensor is installed in an untrusted location for monitoring a particular PQ—eg. voltage.
2. Whenever the user needs to collect data from the PUF sensor. The user randomly selects a challenge **C** and sends it to the PUF sensor. The PUF sensor is stimulated by the **C** and sends the $\mathbf{R}^{\mathrm{PQ_j}}$ back to the user.
3. The user compares all $\mathbf{R}^{\mathrm{PQ}}$s saved in the database to $\mathbf{R}^{\mathrm{PQ_j}}$ corresponding to the **C**. Only the $\mathbf{R}^{\mathrm{PQ_j}}$ stored in the database will match to the received $\mathbf{R}^{\mathrm{PQ_j}}$. If the user finds one of the saved $\mathbf{R}^{\mathrm{PQ}}$ matches $\mathbf{R}^{\mathrm{PQ_j}}$. Then the $\mathrm{PQ}_j$ is discovered. Otherwise, if none of the saved $\mathbf{R}^{\mathrm{PQ}}$ matches $\mathbf{R}^{\mathrm{PQ_j}}$, this round of authentication sensing is rejected.

**InterPQ** InterPQ is used to evaluate the fractional hamming distance (FHD) among different $\mathbf{R}^{\mathbf{PQ}}$s corresponding to the same challenge applied to the same PUF sensor under different PQs. InterPQ is the mean value of the FHD.

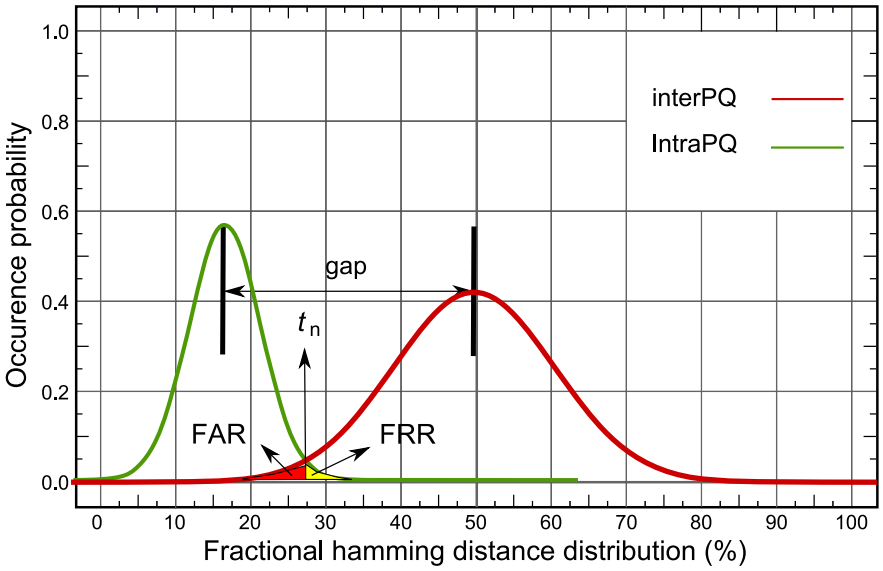


**Fig. 4.** .

**IntraPQ** IntraPQ is used to evaluate the fractional hamming distance (FHD) among regenerated $\mathbf{R}^{\mathbf{PQ}}$s corresponding to the same challenge applied to the same PUF sensor under the same PQ. IntraPQ is the mean value of the FHD.

In step 3, the successfully authentication sensing is guaranteed by the large gap between InterPQ and IntraPQ as shown in Fig. 4. For example, in Fig. 3, the responses under $V_1, V_2, V_3, V_4$ are different for the same challenge referring to InterPQ. In contrast, it is clear that the response will be relatively stable when it is regenerated under the same $V_j$ , $j \in \{1, 2, 3, 4\}$ referring to IntraPQ. The saved $\mathbf{R}^{\mathrm{PQ}}$ can match the received $\mathbf{R}^{\mathrm{PQ_j}}$ when they are generated under the same PQ for the same challenge applied to the same sensor PUF.

To avoid replay attacks, the CRPs are only used once. The number of CRPs produced in a typical ROPUF, used for demonstration of this paper, is not sufficient. However, the number can be significantly increased [19, 20].

## 4 Experimental Demonstration

In this section, we use the public experimental data from five ROPUFs across five Spartan3E S500 FPGAs for validation of the aforementioned PUF sensor to securely sense voltage [38]. Each FPGA consists of 512 ROs to form a ROPUF. Detailed implementation information can be found in [12]. As for the same challenge, the response is reproduced under 0.96 V, 1.08 V, 1.20 V, 1.32 V, 1.44 V respectively, while the temperature is 25°C. Each $\mathbf{R}^{\mathrm{PQ}}$ is re-evaluated 100 times.

### 4.1 Unreliable Responses Selection

If the frequency of $f_i$ and $f_j$ never cross with each other within a specific range, eg. from 0.96 V to 1.44 V. Then the regeneration of the response upon the frequency comparison is always same and show strong tolerance to voltage deviations. In such cases, the response cannot be used to sense the voltage. One task is to find out the unreliable responses based on the frequency difference $\Delta f$ among ROs. If the $\Delta f$ is small among different ROs, the response generated upon them will flip with high probability when the voltage changes. This is the basis of our proposed PUF sensor. In Fig. 5, it shows the frequency distribution under 1.20 V. The mean value is 197.8 MHz. We select ROs satisfying $|f - 197.8| < \Delta f$. It is clear that the number of ROs selected is related to the setting of $\Delta f$. The number will increase as the $\Delta f$ becomes larger.

The reason of selecting unreliable responses under 1.20 V is to increase the gap between InterV—PQ is voltage in this specific experimental demonstration—and IntraV, as shown in Fig. 6. It can be seen that the gap is significantly increased from less than 10% to more than 30%. As a consequence, the length of the response for performing authentication sensing compared with [10] will be significantly shorten .

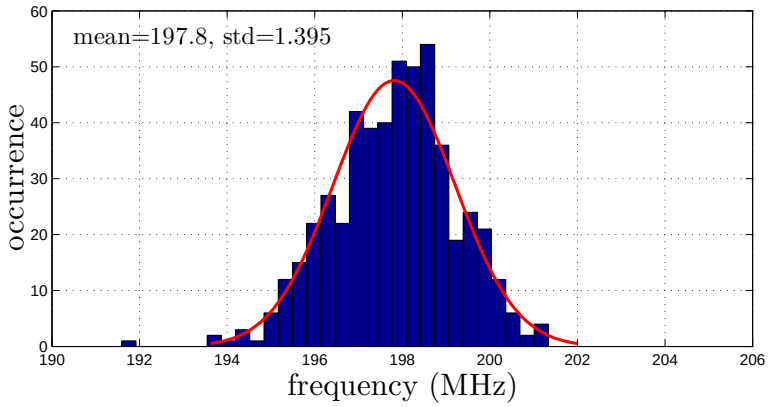


**Fig. 5.** Frequency distribution of 512 ROs in one ROPUF.

Due to the unreliable response is selected under the reference voltage of 1.20V. Therefore, the IntraV under 1.20 V also goes up quickly when the $\Delta f$ shrinks due to the responses are more prone to be influenced by noise. The Fig .7 shows the IntraV under 1.32V as the unreliable response is still selected based on the reference voltage 1.20V. The IntraV is lower compared to Fig. 6 due to the select unreliable response tends to be tolerate some noise as unreliable responses may turn to reliable when the voltage moves from the reference voltage of 1.20V to 1.32V. The Fig. 8 shows the IntraV and InterV of five different ROPUFs. The $\Delta f$ is set to be 0.3 MHz. The IntraV is evaluated under 1.32V. The RO selection is under 1.20V.

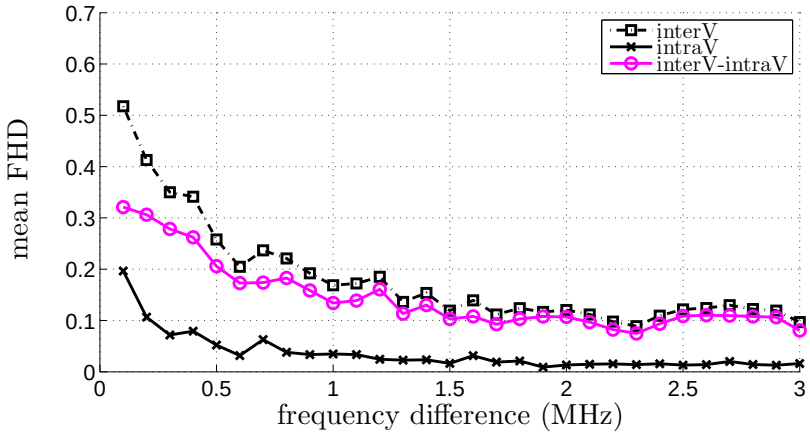


**Fig. 6.** The InterV and IntraV performance for one ROPUF for different $\Delta f$—frequency difference. Unreliable response selection is performed under the reference voltage of 1.20 V. The IntraV is evaluated under 1.20 V

### 4.2 Evaluation of Length of Response Needed

It is important to ensure both of the false acceptance rate (FAR) and false reject rate (FRR) meeting requirements in practice when the PUF sensor employed based on the authentication sensing protocol. The FAR stands for the probability of the user taking the other $\mathrm{PQ}_i$ as $PQ_j$ by mistake. While the FRR stands for the probability of the authenticity $\mathrm{PQ}_i$ is falsely rejected, see Fig. 4. Multiple bits $n$ response is necessary to guarantee minimizing both the FAR and FRR. If a threshold $t_n$ is predefined, then the FRR and FAR can be respectively derived as [30]:

$$\mathrm{FRR} = 1 - \sum_{i=0}^{t_n} i^{\mathrm{IntraPQ}} (n-i)^{(1-\mathrm{IntraPQ})}, \tag{1}$$

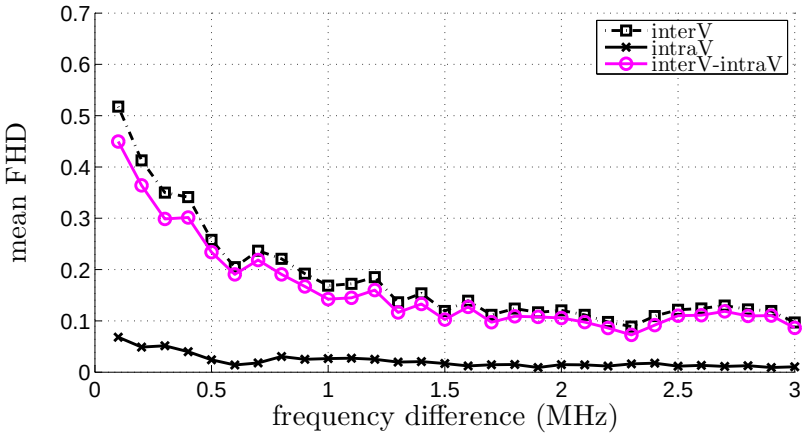


**Fig. 7.** The InterV and IntraV performance for one ROPUF for different $\Delta f$—frequency difference. Unreliable response selection is performed under the reference voltage of 1.20 V. The IntraV is evaluated under 1.32 V.

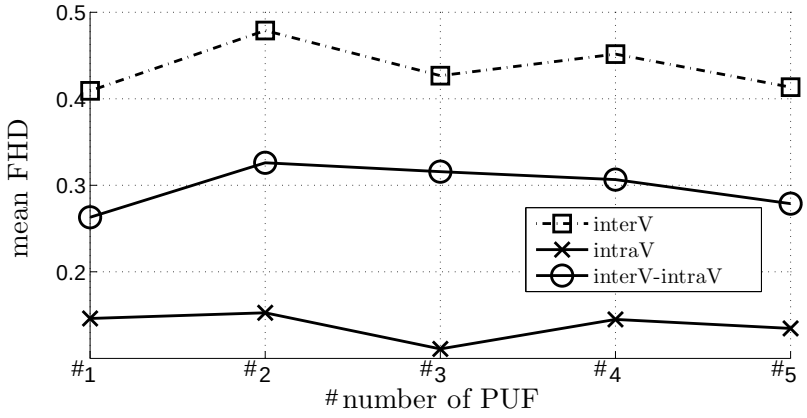


**Fig. 8.** The InterV and IntraV performance across five ROPUFs. Unreliable response selection is performed under the reference voltage of 1.20 V. The IntraV is evaluated under 1.32 V. The $\Delta f$ is 0.3 MHz

$$\mathrm{FAR} = \sum_{i=0}^{t_n} i^{\mathrm{InterPQ}}(n-i)^{(1-\mathrm{InterPQ})}, \tag{2}$$

Where the FRR means the probability of false rejecting the authentic $\mathrm{PQ}_i$ when more than $t_n$ bits out of $n$ bits are the same during authentication sensing. Conversely, the FAR means the probability of false accepting other $\mathrm{PQ}_j$ as $\mathrm{PQ}_i$ when more than $t_n$ bits out of $n$ bits are the same during authentication sensing. It is clear FRR and FAR are undesirable for the authentication sensing since they will introduce errors. Specifically, the FAR expresses the security of an authentication sensing, because a high FAR indicates a high risk of incorrect authentication sensing, which could cause a security issue. The FRR expresses the robustness or usability of the authentication sensing, it indicates a misrejection of the authentic PQ, which will cause the authentication sensing to be impractical.

The FRR and FAR depend on the IntraPQ and InterPQ distribution, and the choose of the identification threshold $t_n$. A high $t_n$ benefits false reject rate but aggravates false acceptance rate, and vice versa for a low threshold. The IntraPQ and InterPQ are usually assumed to follow binomial distribution. It is clear that there is an intersect of FAR and FRR if they are plotted as a function of $t_n$ given fixed $n$, where the error rate of both FAR and FRR are equal. we call this *equal error threshold* as $\mathrm{th}_{\mathrm{EER}}$ and the *equal error rate* as EER. For discrete distribution, FAR and FRR will never be exactly equal for a discrete threshold, and in that case $\mathrm{th}_{\mathrm{EER}}$ and EER are defined as:

$$\mathrm{th}_{\mathrm{EER}} = \mathrm{argmin}_{\mathrm{th}}\{\max\{\mathrm{FAR}_{\mathrm{th}}, \mathrm{FRR}_{\mathrm{th}}\}\}, \tag{3}$$

$$\mathrm{EER} = \max\{\mathrm{FAR}(\mathrm{th}_{\mathrm{EER}}), \mathrm{FRR}(\mathrm{th}_{\mathrm{EER}})\}, \tag{4}$$

In Talbe. 1, we give a quantitative evaluation of $n$—minimal length of response to meet the EER, and $t_n$ of PUF sensor under different IntraPQ and InterPQ determined by $\Delta f$ as shown in Fig. 6. The PQ in this table is voltage.

As can be seen from Table. 1, necessary length of $n$ is decreasing as the $\Delta f$ is decreasing. This indicates the practicability of the authentication sensing and the importance of the implementation of proposed unreliable response selection.

**Table 1.** Quantitative evaluation of necessary length of responses for authentication sensor under different IntraPQ and InterPQ determined by $\Delta f$.

| | | | EER $< 10^{-2}$ | | | | EER $< 10^{-4}$ | | | | EER $< 10^{-6}$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\Delta f$ MHz | IntraPQ | InterPQ | $n$ | $\mathrm{th}_{\mathrm{EER}}$ | $\mathrm{FAR}^*$ | $\mathrm{FRR}^*$ | $n$ | $\mathrm{th}_{\mathrm{EER}}$ | $\mathrm{FAR}^*$ | $\mathrm{FRR}^*$ | $n$ | $\mathrm{th}_{\mathrm{EER}}$ | $\mathrm{FAR}^*$ | $\mathrm{FRR}^*$ |
| 3 | 1.62% | 9.68% | 146 | 7 | −2.00 | −2.02 | 383 | 18 | −4.00 | −4.21 | 623 | 29 | −6.00 | −6.27 |
| 2 | 1.34% | 12.04% | 93 | 5 | −2.01 | −2.12 | 235 | 12 | −4.01 | −4.14 | 380 | 19 | −6.03 | −6.04 |
| 1 | 3.48% | 16.88% | 98 | 9 | −2.02 | −2.12 | 247 | 22 | −4.04 | −4.16 | 397 | 35 | −6.03 | −6.10 |
| 0.5 | 5.21% | 25.80% | 63 | 9 | −2.04 | −2.28 | 148 | 20 | −4.05 | −4.03 | 244 | 33 | −6.01 | −6.21 |
| 0.3 | 7.16% | 31.00% | 41 | 8 | −2.02 | −2.11 | 106 | 20 | −4.08 | −4.23 | 167 | 31 | −6.04 | −6.02 |

Note: the $^*$ symbol means value is from log10.

### 4.3 Improve Resistance against Modeling Attacks

Current modeling attacks built upon machine learning techniques only use the CRP to train a model to achieve a high prediction rate of the $\mathbf{R}$ for the unused $\mathbf{C}$. Such model does not take a specific PQ into consideration during training the model. Generally, the unreliability of the PUF is considered as a flaw with regarding to the modeling attacks since the prediction rate of the model only needs to exceed the reliability of the PUF, then the model is able to impersonate the physical PUF [6, 8]. In contrast, we show the unreliability of PUF is actually improve resistance against modeling attacks that seems intuitively controversy to previous conclusions.

Note the PUF sensor treat both challenge and PQ as input to determine the response. In such cases, if the model only solely takes the challenge as the input to train the model. Then the user/verifier can still distinguish the model from the physical device even the prediction rate of the model is sufficient high thanks to the model is unable to predict $\mathbf{R}^{\mathrm{PQ_j}}$ accurately. For example, assume the adversary trains the model utilizing CRPs measured/eavesdropped under nominal condition—$\mathrm{PQ}_i$. It is clear that the model is unable to succefully predict the $\mathbf{R}^{\mathrm{PQ_j}}$ even for the same challenge resulting in $\mathbf{R}^{\mathrm{PQ_i}}$, where $i \neq j$, let alone predicts $\mathbf{R}^{\mathrm{PQ_j}}$ for a different $\mathbf{C}$ with high accuracy.

Consequently, the adversary have to take the PQ into consideration, which inevitably increases the number of CRPs to train the model and may also increases the complexity of machine learning algorithms. In other word, the unreliable response helps to increase the resistance against modeling attacks.

## 5 Conclusion

In this paper, we present a novel approach to treat the PUF as a sensor through utilizing its unreliability. The PUF sensor secures remotely sensing taken in an untrusted locations even when the communication is through insecure digital channels. We provide an authentication sensing protocol applicable to PUF sensors. In the authentication protocol, there is no actual sensed values involved prevents measurement spoofing from the adversary. Moreover, we propose a method to fast the selection of the unreliable responses to speed the enrollment phase up and to greatly short the length of the response during authentication sensing phase. The quantitative analysis of length of response is carried out based on the experimental results. Further, the unreliability of the PUF is actually increase the resistance against modeling attacks when the unreliable responses are utilized appropriately.

## References


1. 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.
2. G. E. Suh and S. Devadas, "Physical nclonable functions for device authentication and secret key generation," in *Proceedings of the 44th Annual Design Automation Conference*. ACM, 2007, pp. 9–14.
3. R. Anderson, *Security Engineering*. John Wiley & Sons, 2008.
4. O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," in *USENIX Workshop on Smartcard Technology*, vol. 12, 1999, pp. 9–20.
5. R. Maes, A. Van Herrewege, and I. Verbauwhede, "PUFKY: A fully functional puf-based cryptographic key generator," in *Cryptographic Hardware and Embedded Systems*–CHES. Springer, 2012, pp. 302–319.
6. D. Lim, "Extracting secret keys from integrated circuits," Ph.D. dissertation, Massachusetts Institute of Technology, 2004.
7. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 2010, pp. 237–249.
8. 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 Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1876–1891, 2013.
9. 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.
10. 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 *36th IEEE Symposium on Security and Privacy*, 2015, DOI: 10.1109/SP.2015.12.
11. B. Fisch, D. Freund, and M. Naor, "Physical zero-knowledge proofs of physical properties," in *Advances in Cryptology–CRYPTO*. Springer, 2014, pp. 313–336.
12. A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A large scale characterization of RO-PUF," in *IEEE International Symposium on Hardware-Oriented Security and Trust (*HOST),, 2010, pp. 94–99.
13. A. Maiti and P. Schaumont, "Improved ring oscillator PUF: an FPGA-friendly secure primitive," *Journal of Cryptology*, vol. 24, no. 2, pp. 375–397, 2011.
14. R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.
15. B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.
16. D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.
17. U. Ruhrmair and M. Van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *IEEE Symposium on Security and Privacy (*SP), 2013, pp. 286–300.
18. A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *Proc. IEEE Int. Conference on Field Programmable Logic and Applications*, 2009, pp. 703–707.
19. A. Maiti, I. Kim, and P. Schaumont, "A robust physical unclonable function with enhanced challenge-response set," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 333–345, 2012.
20. M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2014, DOI:10.1145/2593069.2593072.
21. J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon PUFs and recent advances in ring oscillator PUFs," *Journal of Computer Science and Technology*, vol. 29, no. 4, pp. 664–678, 2014.
22. D. E. Holcomb, W. P. Burleson, and K. Fu, "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in *Proceedings of the Conference on RFID Security*, vol. 7, 2007.
23. Holcomb, Daniel E, W. P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.
24. Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, 2008.
25. R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," in *3rd Benelux Workshop on Information and System Security (*WISSec), vol. 17, 2008.
26. V. van der Leest, G.-J. Schrijen, H. Handschuh, and P. Tuyls, "Hardware intrinsic security from D flip-flops," in Proceedings of the fifth ACM Workshop on Scalable trusted computing, 2010, pp. 53–62.
27. S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly PUF protecting ip on every FPGA," in *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 67–70.
28. M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based PUF," in *Proc. IEEE Int. Sym on Circuits and Systems* (ISCAS), 2011, pp. 2071–2074.

29. R. Kumar and W. Burleson, "On design of a highly secure PUF based on non-linear current mirrors," in *Proc. IEEE Int. Sym on Hardware-Oriented Security and Trust* (HOST), 2014, pp. 38–43.
30. M. Roel, "Physically unclonable functions: Constructions, properties and applications," Ph.D. dissertation, University of KU Leuven, 2012.
31. C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of IEEE*, vol. 102, pp. 1126–1141, 2014.
32. 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 Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 921–932, 2014.
33. Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "mrPUF: A novel memristive device based physical unclonable function," in *13th International Conference on Applied Cryptography and Network Security*, 2015.
34. 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.
35. 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 Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1630–1642, 2015.
36. Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," IEEE Access, 2015, In press.
37. A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Embedded Systems Design with FPGAs*. Springer, 2013, pp. 245–267.
38. http://rijndael.ece.vt.edu/variability/main.html.