A fully digital physical unclonable function based temperature sensor for secure remote sensing

Cao, Yuan; Guo, Yunyi; Liu, Benyu; Ge, Wei; Zhu, Min; Chang, Chip Hong

2018

Cao, Y., Guo, Y., Liu, B., Ge, W., Zhu, M., & Chang, C. H. (2018). A fully digital physical unclonable function based temperature sensor for secure remote sensing. Proceedings of 2018 27th International Conference on Computer Communication and Networks (ICCCN). doi:10.1109/ICCCN.2018.8487347

<https://hdl.handle.net/10356/143632>

<https://doi.org/10.1109/ICCCN.2018.8487347>

© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: <https://doi.org/10.1109/ICCCN.2018.8487347>.

Downloaded on 26 Apr 2023 19:43:26 SGT

A Fully Digital Physical Unclonable Function based Temperature Sensor for Secure Remote Sensing

(Invited Paper)

Yuan Cao¹, Yunyi Guo², Benyu Liu², Wei Ge², Min Zhu³, and Chip-Hong Chang⁴

¹College of Internet of Things Engineering, Hohai University, Changzhou, China

²National ASIC System Engineering Research Center, Southeast University, Nanjing, China

³Wuxi Research Institute of Applied Technologies Tsinghua University, Wuxi, China

⁴School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

Abstract—Turnkey solutions that combine energy-efficient remote sensing and secure communication of telemetry are desirable in data collection, risk control and situation appraisal with the large scale deployment of resource constrained Internet of Things devices. In this paper, a new low-cost physical unclonable function (PUF) based temperature sensor for secure remote temperature sensing is proposed. The design exploits the approximately linear positive temperature coefficient of CMOS inverter in super-threshold operation to calibrate the running frequency of ring oscillator (RO) in a reconfigurable RO PUF at different temperature. The RO frequency corresponding to the sensed temperature is fed into a randomizer seeded by the input challenge to select new RO pairs for comparison to generate a random, unique and physically unclonable digital tag, which is valid for a selected input challenge to a target device at a particular temperature. Using only standard logic cells and a very simple structure, the proposed temperature sensor can be easily implemented on FPGA and integrated into other digital systems. It protects the integrity of the sensed information by preventing falsified sensor data and masquerade sensing node. The FPGA implementation of our proposed design has demonstrated the feasibility of making a trust temperature telemetry system out of PUF.

I. INTRODUCTION

Recently years have witnessed the rapid advancements of the smart temperature sensors and low-cost temperature telemetry system. Remote temperature sensing, leveraging the Internet of Things (IoT) devices and communications, pervades a broad range of new applications, from the industrial temperature monitoring to the smart homes, smart vehicles, virtual reality, e-health, etc. [1]–[3]. As temperature sensors are nodes of a distributed network and the sensed temperature is sometimes sensitive or confidential, the sensors are expected to provide a certain level of trust [4], [5]. An example is the Exelon Nuclear’s Limerick Generating Station in Montgomery County, Pennsylvania, America where temperature sensors are employed with the wireless communication technology to monitor the fans that are used to exhaust turbine enclosures [6]. A sophisticated attacker can spoof the temperature sensor inside one of the turbines to make the control center believe that the internal temperature is significantly lower than it actually is. The cooling system for the turbine will stop working, resulting in overheating. This could be real as recent reports from *New York Times* and *Bloomberg* show that the

hackers have already successfully penetrated the Wolf Creek nuclear facility [7]. Moreover, as the smart temperature sensors in IoT are resource-constrained in nature and usually remotely deployed in open areas, it is easier for the adversaries to tamper the devices to perform fraudulent attacks [8], [9].

To ensure the integrity of the sensor and the sensed information, effort has been made to develop new or adapt authentication schemes for low cost and resource-constrained IoT devices. Many lightweight key-based cryptography algorithms have been proposed [10]–[12]. Unfortunately, these methods are essentially software rooted with mechanism designed originally for online services. They cannot be practically scaled for hardware implementation with limited programmability and scarce memory resources. Besides, almost all lightweight authentication schemes rely on cryptographic primitives that assume the secrecy of a shared “key” between the prover and the verifier. While the shared secret is easier to protect at the server end, the key stored in the device local memory is susceptible to invasive and semi-invasive attacks [13]. Physical unclonable function (PUF) based sensing schemes have been proposed to authenticate a physical sensing device in a lightweight manner without the need for safekeeping any secret key locally [4], [5], [14], [15]. A PUF is a circuit that can directly harness the parametric mismatches arising from the uncontrollable and unpredictable device manufacturing process variations to generate a reliable and unique digital fingerprint of the device [16]. Its underlying challenge-response generation mechanism can be extended to associate a physically sensed quantity with a “witnessed object” to provide a virtual proof of reality, a notion that was first introduced in [17]. This forms the basis of many sensor PUFs that make their response generation mechanism also dependent on an external physical property.

In view of the potential abuse of temperature telemetry, we propose a novel fully digital PUF based temperature sensing scheme to secure temperature telemetry. It exploits the temperature sensitivity of ring oscillator (RO) in a reconfigurable RO PUF. The preliminary contributions of this work can be summarized as follows:

- Most of the smart temperature sensors are full-custom designed with handcrafted critical components [1]. It is not directly portable across technology nodes for integra-

tion with other VLSI designs. Our proposed PUF based temperature sensor is a fully digital design. Using only standard logic cells and simple structure, it can be easily scaled and designed as a reusable IP core for seamless integration into a complete telemetric system.

- The RO of the RO PUF is reused as a sensing component of environmental temperature. There is currently no additional overhead needed to realize this basic function. Additional components may be added to improve the sensing accuracy and remove noise from the proof-of-concept prototype in the near future.
- A unique authentication protocol based on the coherent tagging of temperature by the response of PUF has been proposed to validate the temperature telemetry as well as identifying the origin of sensing.
- The proposed design has been successfully implemented in FPGA. The measurement results demonstrate the feasibility and efficiency to convert an RO PUF into a lightweight trust temperature sensor for secure remote sensing and temperature telemetry.

The remaining of this paper is organized as follows. Section II presents the background knowledge of the proposed PUF based sensor. The circuit implementation and the authentication scheme are elaborated in Section III. Measurement results are presented and discussed in Section IV. The conclusion is drawn in Section V.

II. BACKGROUND

A. PUF

In the last fifteen years, many PUFs have been proposed and used as a lightweight but secure cryptography primitive in device authentication/identification, key management and device counterfeiting [16], [18]–[21]. It is essentially an extension of biometrics towards physical objects. To be specific, PUF possesses qualities which cannot be obtained from cryptographic deductions, but requires a physical basis to establish them, the most noteworthy being physical unclonability. It extracts the unique digital signatures from the unpredictable and uncontrollable process variations inherent in chip manufacturing. The inputs and outputs of PUF circuits are typically called the challenges and responses, respectively. The mapping of challenge and response pairs (CRPs) is unique to each PUF instance. Unlike storing the confidential key in a non-volatile memory, PUF keeps the secret into its innate structure. Any invasive or semi-invasive attacks will likely to affect the subtle physical mismatches of the chip's original structure from which the challenge-response pairs were measured during the enrollment phase. Therefore, the key obtained by the attacker will be invalid. From this perspective, PUF also possesses tamper-awareness as the tampered chip will no longer be authenticable.

RO PUF is a popular PUF which has proven to be more robust and less constrained by layout than many other delay based PUFs [22]. The basic RO PUF architecture [23] is made of two n -bit multiplexors, two frequency counters, one

Fig. 1. Architecture of a typical RO PUF.

Fig. 2. Fundamental difference between standard PUF and sensor PUF.

comparator and n ROs, as shown in Fig 1. Each RO contains an odd number of inverters in a feedback loop. Due to process variations, each RO in the PUF may be characterized by a slightly different oscillation frequency. A challenge is applied to the multiplexors to select a pair of ring oscillators to compare their oscillation frequencies. The output is 0 or 1 depending on which RO has a higher oscillation frequency. RO PUF is FPGA implementation friendly as it is less sensitive to the routing distance of the ROs' outputs to the counters. High reliability can also be archived by allowing the ROs to "ring" for a longer time to amplify the small frequency difference [13].

B. Sensor PUF

The notion of sensor PUF is introduced in [4]. Fig. 2 illustrates the concept of sensor PUF. It differs from conventional PUFs in that it introduces an extra input, which is a physical quantity being sensed, besides the binary challenge. A sensor PUF can be expressed as a black box function with the output response R given by:

$$R = PUF(C, P) \quad (1)$$

where C is the challenge, and P is the physical quantity that can be indirectly and safely sensed by corresponding electrical circuit within the PUF. Both the sensor and its sensed data can be authenticated concurrently by validating the response with similar challenge-response protocol between the prover and the verifier as in normal PUF.

C. Temperature Dependency of ROs Frequency

The oscillation frequency of a RO is inversely proportional to the propagation delay t_d of each inverter stage. The first order estimate of t_d can be expressed as [24]:

$$t_d = \frac{(L/W)C_L}{\mu C_{OX}(V_{GS} - V_T)} \ln\left(\frac{1.5V_{DD} - 2V_T}{0.5V_{DD}}\right) \quad (2)$$

where W , L , V_{GS} , C_{OX} , V_T , μ , C_0 and V_{DD} are the effective channel width and length, gate-to-source voltage, oxide capacitance, threshold voltage, charge carrier mobility, total load capacitance and the power supply voltage, respectively. The temperature dependent parameters, V_T and μ , are expressed as [25]:

$$V_T(T) = V_T(T_0) - \sigma(T - T_0) \quad (3)$$

$$\mu(T) = \mu(T_0)\left(\frac{T}{T_0}\right)^\kappa \quad (4)$$

where T_0 is the reference temperature. κ and σ , are respectively the mobility temperature exponent in the range of 1.2~2 and the threshold voltage temperature coefficient in the range of 0.5~3mV/K.

The threshold voltage $V_T(T)$ decreases with temperature, resulting in a higher running frequency. The mobility of charge carriers also decreases with temperature, but this will slow down the oscillation frequency as the temperature increases. For device operating in the super-threshold region, the reduction in carrier mobility with temperature is more prominent than the reduction in threshold voltage. Consequently, the delay of an inverter gate in FPGA exhibits a positive temperature dependence relation [19].

III. PROPOSED PUF BASED TEMPERATURE SENSOR

In this section, the design, operating principle and authentication protocol of the proposed PUF based temperature sensor are detailed.

A. Circuits Implementation

Fig. 3 shows the block diagram of the proposed PUF based temperature sensor. It consists of three main parts: one N -bit linear feedback shifter register (LFSR), one N -bit reconfigurable RO and two digital counters. An LFSR is a shift register that takes a linear function, typically XOR, of selected bits from a previous state as an input for the computation of its next state. In our design, a maximum length LFSR is employed to introduce the sensed temperature as an input variable into the PUF response generation. The key component of the proposed sensor PUF is the reconfigurable RO, which is used for both temperature sensing and as generator of unique temperature dependent device identity. The schematic of the reconfigurable RO is shown in the bottom of Fig. 3. It is formed by a NAND gate and N (N is an even number) inverter stages. In each inverter stage, C_i ($i = 0, 1, 2, \dots, N-1$) selects either the upper or the lower inverter. When EN is asserted, the NAND is equivalent to an inverter, resulting in an $N+1$ stage RO. 2^N different oscillation paths can be selected by a different N -bit vector $\{C_0 \sim C_{N-1}\}$. The lengths of the two digital counters should be longer than the product of the RO's frequency and counting time to avoid overflow. Counter 1 is a standard unidirectional counter while Counter 2 is a bidirectional counter, which can be configured as either an up or a down counter with a binary control signal.

Fig. 3. Block diagram of the proposed PUF based temperature sensor.

B. Telemetry Tag Generation

Fig. 4 illustrates the operating principle of the proposed PUF based temperature sensor. Two phases, namely temperature measurement and temperature hashing, are involved in the tagging of temperature telemetry recorded by the PUF. In the temperature measurement phase, an arbitrarily selected challenge is fed into the N -bit LFSR as an initialization seed. The N -bit outputs $\{C_0 \sim C_{N-1}\}$ of the LFSR (which cannot be all zeros since this is forbidden by the LFSR) is then used as an input challenge to select a RO path from the reconfigurable RO. To generate an oscillation frequency from the selected RO path, the EN signal is pulled high. The oscillation frequency f is measured by clocking Counter 1 with the output of the reconfigurable RO for a time interval t . The recorded count $D(T)$ in the counter has a direct correspondence to the sensed operating temperature of the device. The challenge $\{C_0 \sim C_{N-1}\}$ should select an RO, which has a higher temperature sensitivity than the others in the enrollment phase (see Section III-C1). In the temperature hashing phase, another randomly generated challenge $challenge'$ is applied to the LFSR for initialization. A new vector $\{C_0 \sim C_{N-1}\}'$ is generated by the LFSR after $D(T)$ clock cycles. This vector is used to select a new RO path in the reconfigurable RO. The frequency f' of the new RO triggers Counter 2 to count up for the same time interval t . The LFSR is then shifted by another $D(T)$ clock cycles to generate a random vector $\{C_0 \sim C_{N-1}\}''$ to select a different RO with a new frequency f'' . Counter 2 is now configured in the count-down mode to count the number of cycles of f'' for the same time interval t . The value stored in Counter 2 represents the difference between f' and f'' . The sign bit of Counter 2 is output as a response bit. Multiple response bits can be generated by shifting the LFSR by $D(T)$ cycles multiple times in the temperature hashing phase. n independent response bits can be generated after $2n \times D(T)$ cyclic shifts of LFSR.

Fig. 4. Operation flow for the generation of telemetry tag by the proposed temperature sensing PUF.

C. Proposed Authentication Scheme

To protect the integrity of temperature telemetry based on the proposed PUF based sensing, a trust protocol is proposed. The device to be authenticated is first enrolled and calibrated before it is deployed in the field for future authentication by an authorized remote server of the monitoring center.

1) *Enrollment Phase*: The enrollment is performed before the sensor is deployed to collect the necessary information of the device for authentication. The procedure is depicted in Algorithm 1. Sampling tests are performed to select an RO that has a very high temperature sensitivity and good linearity. The challenge for this RO is denoted as α . The temperature is measured by this RO at different temperature T_j to obtain the digitized temperature output $D(T_j)$. A set of random numbers to be used as prospective challenges for future device authentication is generated. Each such challenge, designated as α_i , is applied to all the PUF based sensors under different temperature T_j to generate a unique response $\gamma_{i,j}$. All the mappings of $[\alpha_i, D(T_j), \gamma_{i,j}]$ are securely stored in a trusted server database. After this, the PUF based temperature sensor is deployed in the field (where the operating environment may be potentially open and hostile) for remote temperature sensing. No further calibration is needed as the enrollment process itself serves as a form of sensor calibration [5].

2) *Authentication Phase*: This phase enables the monitoring center to authenticate the trust sensor after its deployment. The authorized user requests the enrolled α and a randomly challenge α_i for the device i to be authenticated from the server and sent them to the device. The device applies the challenge α to sense the temperature. The sensed temperature T_j is recorded in Counter 1 as $D(T_j)$. Then the device evaluate the PUF response $\gamma'_{i,j}$ with the challenge α_i and sensed temperature $D(T_j)$. Then $\gamma'_{i,j}$ together with $D(T_j)$ is sent back to the server for validation. If the received $\gamma'_{i,j}$ matches $\gamma_{i,j}$ stored in the database, the sensor and its sensed temperature are authenticated. Otherwise, the telemetry is denied due either

Algorithm 1 Enrollment

```

1: for PUF Device  $d$  in DeviceList do
2:    $\alpha \leftarrow$  Challenge selects the most temperature sensitive RO
3:   for Temperature  $T_j$  in MeasurementRange do
4:      $D(T_j) \leftarrow$  Measure the temperature with RO selected by  $\alpha$  in the controlled environment
5:   end for
6: end for
7: for PUF Device  $d$  in DeviceList do
8:   Challenge  $\alpha_i \leftarrow$  random number generator
9:   for Temperature  $T_j$  in MeasurementRange do
10:    Response  $\gamma_{i,j} \leftarrow \text{PUF}(\alpha_i, D(T_j))$ 
11:   end for
12:   Server  $\leftarrow$  store enrollment entry  $[\alpha_i, D(T_j), \gamma_{i,j}]$ 
13: end for

```

Algorithm 2 Authentication

```

1: Challenge  $\alpha \leftarrow$  read the challenge temperature measurement from the server database
2:  $D(T_j) \leftarrow$  sense the environmental temperature
3: Challenge  $\alpha_i \leftarrow$  read a random sequence of challenges from the server database
4: Response  $\gamma'_{i,j} \leftarrow \text{PUF}(\alpha_i, D(T_j))$ 
5: Send  $[\gamma'_{i,j}, D(T_j)]$  to the server
6:  $T \leftarrow$  match  $[\alpha_i, D(T_j), \gamma_{i,j}]$  and  $[\alpha_i, D(T_j), \gamma'_{i,j}]$ 
7: Authentication successful  $\leftarrow T = \text{true?}$ 

```

to the unauthentic device or untrusted telemetry. The used sequence of challenges will be deleted from the server to prevent replay attack.

IV. EXPERIMENTAL RESULTS

The proposed secure PUF based temperature sensor can be fully implemented in digital logic. Hence its functionality and performance can be validated and evaluated by FPGA-based implementation without the need for a costly full-custom design. The setup of the experiment is shown in Fig. 5. The FPGA bitstream of the prototype design is programmed into the Virtex-7 XC7VX690T-2FFG1761C FPGA chip of an Xilinx VC709 evaluation board. The control signals are generated from a PC and communicated with the FPGA board is performed through a UART. The collected data are then processed with MATLAB scripts. An Agilent DSO7034A digital storage oscilloscope with 2 GSa/s is used to capture the RO's output frequency and verify the timing of the system.

A. Temperature Sensing

To evaluate the performance of the proposed design as a temperature sensor, the programmed FPGA is placed in the temperature chamber KeHeng FCD-3000. The internal temperature of the chamber is calibrated by a Pt100 temperature sensor. The temperature measurement of the proposed sensor was done every degree from 25 to 50 °C. Counter 1 and 2 are both 32 bits long. The measured oscillation frequencies of

Fig. 5. Experimental setup.

TABLE I
HARDWARE RESOURCES, MEASUREMENT ERRORS AND RESOLUTIONS FOR THE PROPOSED SENSOR WITH DIFFERENT LENGTHS OF RECONFIGURABLE ROs.

Length of RO	33	65	257
Resource (LUT)	178	242	626
Error (°C)	-1.4~1.4	-1.3~1.6	-1.3~1.6
Resolution (°C)	0.05	0.08	0.36

different lengths of RO versus the temperature is plotted in Fig. 6. The frequency decreases with temperature and satisfies the theoretically approximated linear relationship presented in Section II-C. From the curve-fitting results obtained in Fig. 6, we can conclude that the shorter the RO, the higher the temperature resolution as the oscillation frequency is higher. This is achieved at the expense of a longer counting time and more power consumption. Moreover, the self-heating effect is worse at the higher frequency, which limits the accuracy of the sensor. The used hardware resources, measurement errors, and targeted resolutions for ROs with different number of inverter stages are summarized in Table I. The dynamic power consumptions for the three implementations reported by Vivado [26] are all below 1mW. As the measurement errors are almost identical, 33-stage RO is used for the remaining evaluations.

B. PUF metrics

1) *Uniqueness*: Uniqueness is a standard metric to characterize how different are the CRPs generated by a specific PUF instance from those generated by other instances. It is usually estimated by the inter-die Hamming distance (HD) as follows:

Fig. 6. Measured oscillation frequencies for different lengths of RO and their best-fit linear curves.

$$U = \frac{2}{P(P-1)} \sum_{u=1}^{P-1} \sum_{v=u+1}^P \frac{HD(R_u, R_v)}{n} \times 100\% \quad (5)$$

where $HD(\cdot)$ measures the Hamming distance between two vectors. R_u and R_v are the n -bit responses produced by two different PUF instances, u and v , respectively by applying the same challenge under the same temperature. P is the total number of PUF instances. The ideal value of the uniqueness is 50%, which provides the largest distinguishability among different PUF chips. From the 128 CRPs collected from six FPGAs, the uniqueness is calculated to be 51.82% with a standard deviation of 8.56%. Fig 7 shows the histogram of the measured inter-die HDs.

2) *Diffuseness*: In the proposed design, the CRP behaviors are expected to change as much as possible when the sensed temperature changes. Diffuseness is defined to estimate how different are the CRPs for different temperature as [27]:

$$D = \frac{2}{Q(Q-1)} \sum_{i=1}^{Q-1} \sum_{j=i+1}^Q \frac{HD(R_i, R_j)}{n} \times 100\% \quad (6)$$

where R_i and R_j are the n -bit responses produced by one PUF instance at two different temperature, i and j , respectively, with the same applied challenge. Q is the total number of the measured temperature. Similar to uniqueness, the ideal diffusion should be 50%. The mean diffusion is calculated to be 51.46% with a standard deviation of 6.41% from 128 CRPs at seven temperature points taken from 27 to 45 °C with a step size of 3 °C, as shown in Fig 8. .

Fig. 7. Frequency distribution of the measured inter-die HDs at the room temperature (27 °C).

Fig. 8. The measured diffuseness.

3) *Reliability*: The reliability measures how stable a PUF can reproduce the CRPs under different operating conditions. It is estimated by the bit error rate (BER), which is calculated by the intra-die HD. An n -bit response R_i to a random challenge at the normal operating condition is extracted as the reference. The same challenge is then applied k times to the same PUF instance under either the same (for temporal stability at each operating condition) or different operating conditions (for robustness against changes in specific operating condition) to obtain k responses, $R_{i,j}$ for $j = 1, 2, \dots, k$. The reliability S of the i -th PUF is calculated by:

$$S = 1 - BER = 1 - \frac{1}{k} \sum_{j=1}^k \frac{HD(R(T)_i, R(T)_{i,j})}{n} \times 100\% \quad (7)$$

The reliability is usually evaluated under different supply voltages and temperature. The oscillation frequency of an RO with its transistors operating in super-threshold region is

Fig. 9. BER of the CRPs generated by the proposed PUF at different temperature.

more sensitive to temperature than supply voltage variations. Moreover, as the VC709 board uses power regulators and PMBus compliant digital PWM system controllers from Texas Instrument digital power to supply the core and auxiliary voltages [28], the power supply is stable against large fluctuations of the supply voltages. Therefore, only temperature reliability is evaluated. Since we use PUF response for tagging the temperature sensed by the device, the PUF response to the same challenge should change with temperature but remains stable temporally at the same temperature. 200×128 random challenges each of 32 bits are generated from each PUF instance to obtain 200 128-bit responses. The same challenges are applied 10 times to each PUF instance at each temperature T sampled over the temperature range from 27 °C to 45 °C. Five PUF instances are tested. The BER of the native PUF responses for each measured temperature is shown in Fig. 9. The worst-case BER is 1.72% at 42 °C.

4) *Randomness*: The randomness of the coherent PUF based temperature tag is evaluated by the NIST Pub 800 statistical test suite with the recommended settings [29]. 10M CRPs are collected as the input binary stream for the NIST tests. The results are shown in Table II. The uniform distribution from column C1 to C10 indicates a uniform frequency distribution of the various P-values. The 11th column is the P-value calculated via a Chi-square test. A P-value greater than 0.01 is required to consider an arbitrary information source as random with a confidence level of 99% [29]. Our proposed design consistently exhibits high P-values (> 0.01) for each NIST test. The 12-th column indicates passing rate of the test sequences. The results support the randomness of the bit sequence extracted by the proposed design is sufficient for device-specific temperature tagging.

C. Security Analysis

In this subsection, we analyze a few possible attacks for the proposed PUF based temperature sensor.

TABLE II
NIST TEST RESULTS ON BIT SEQUENCES GENERATED BY OUR PROPOSED PUF.

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P VAL	PROP	TEST
1	0	2	2	0	0	1	3	0	1	0.350485	10/10	Frequency
0	0	2	0	2	3	0	3	0	0	0.066882	10/10	BlockFrequency
1	1	1	0	2	2	0	0	1	2	0.739918	10/10	CumulativeSums
1	0	1	1	0	2	0	1	2	2	0.122325	10/10	Runs
1	0	0	1	1	1	0	1	2	3	0.534146	10/10	LongestRun
1	1	2	1	1	1	0	1	0	2	0.911413	10/10	FFT
1	2	0	2	1	0	1	2	1	0	0.739918	10/10	NonOverlappingTemp.
2	2	0	0	0	3	1	1	0	1	0.350485	10/10	Serial
3	1	1	1	0	1	0	1	0	2	0.534146	9/10	LinearComplexity

1) *Reply Attack*: An adversary cannot spoof the server by simply replaying a message in the authentication phase, because the challenge is randomly chosen or generated from a random number generator. Even if the adversary can intercept the challenge, he will not be able to produce the correct tag to a falsify the telemetry without the PUF. To enhance the security, the used sequence of challenges can be deleted from the database.

2) *Cloning Attack*: It is impossible for the attackers to duplicate another device that shares the same challenge-response behavior as the proposed PUF to masquerade as the authentic device in the network even if the schematic, operation and other details are known to the attacker. This is due to the physical unclonability of the reconfigurable RO PUF.

3) *Machine Learning Attack*: The proposed PUF based temperature sensor is believed to be more resilient to machine learning attack. As the sensed temperature is an integral part of the challenge-response generation process, the entropy of the entire tagging system has been increased. The machine learning tools have to model the PUF's behaviour at different temperature. To achieve a reasonably high predication accuracy, even if it is feasible, enormously large training samples and training time are expected.

4) *Physical Attack*: Unlike the traditional cryptographic algorithm based authentication method, no shared secret is kept in the local non-volatile memory of the sensing device. The adversary cannot obtain the sensitive information by physical attack such as memory probing, fault injection, etc. [13]. Due to the tamper awareness of PUF, such attacked device will be easily discovered before the attacker can reap any benefit from further attempt to make use of the compromised device even if it is still functional as a temperature sensor after the attack.

V. CONCLUSION

This paper presents a novel low-cost all-digital PUF based temperature sensor. The oscillation frequency of the free running RO in a reconfigurable RO PUF against temperature variation is studied and used to sense the environmental temperature. The temperature is digitized and fed back to the reconfigurable RO PUF to produce a unique response. The response can be used to authenticate the sensor device and the sensed temperature. The FPGA implementation has demonstrated the proposed design consumes very little power

and hardware resources, which is very attractive to resource-constrained IoT devices. The proof of concept prototype can be improved in several aspects. In our future work, we will delve into the salient design parameters to improve the resolution and linearity of temperature. Ancillary adaptive control or trimming circuit will be considered to achieve very high temperature resolution. Extensive experiments will be performed on different types of FPGAs to develop a systematic methodology for temperature calibration and enrollment. The design will be implemented on low-cost FPGAs such as Altera ACEX 1K series to afford the collection of more inter-die data for a larger scale evaluation and statistical analysis of the PUF quality and performance. As most of the monitoring sensors are deployed remotely in the harsh environment (e.g., high temperature) and active for a long period of time, the impact of aging effect on sensors performance will also be studied.

VI. ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant No. 61601168), the Singapore Ministry of Education MOE AcRF Tier I grant no. MOE 2018-T1-001-131 and the Fundamental Research Foundation of Shenzhen (Grant No. JCYJ20170302151209762).

REFERENCES

- [1] P. Chen, S. C. Chen, Y. S. Shen, and Y. J. Peng, "All-digital time-domain smart temperature sensor with an inter-batch inaccuracy of -0.7°C $- +0.6^{\circ}\text{C}$ after one-point calibration," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 58, no. 5, pp. 913–920, May 2011.
- [2] A. Davidson, A. Buis, and I. Glesk, "Toward novel wearable pyroelectric temperature sensor for medical applications," *IEEE Sensors Journal*, vol. 17, no. 20, pp. 6682–6689, Oct 2017.
- [3] H. Habibzadeh, A. Boggio-Dandry, Z. Qin, T. Soyata, B. Kantarci, and H. T. Mouftah, "Soft sensing in smart cities: Handling 3vs using recommender systems, machine intelligence, and data analytics," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 78–86, Feb 2018.
- [4] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, June 2010, pp. 112–117.
- [5] Y. Gao, G. Li, H. Ma, S. F. Al-Sarawi, O. Kavehei, D. Abbott, and D. C. Ranasinghe, "Obfuscated challenge-response: A secure lightweight authentication mechanism for puf-based pervasive devices," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, March 2016, pp. 1–6.
- [6] K. Korsah *et al.*, "Instrumentation and controls in nuclear power plants: An emerging technologies update," U.S.NRC, Tech. Rep., 2009. [Online]. Available: <https://www.nrc.gov/docs/ML0929/ML092950511.pdf>
- [7] N. Perlroth, "Hackers are targeting nuclear facilities, homeland security dept. and f.b.i. say," Jul. 2017. [Online]. Available: <https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html>
- [8] R. Maes, R. Maes, and T. U. Darmstadt, "Physically unclonable functions: Constructions, properties and applications," in *Ph.D. thesis, KU Leuven (2012), Ingrid Verbauwhede (promotor)*, 2013.
- [9] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A. R. Sadeghi, and G. Tsudik, "Invited: Things, trouble, trust: On building trust in iot systems," in *2016 53rd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2016, pp. 1–6.
- [10] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, p. 500528, 2006.
- [11] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," *ACM/IEEE IPSN*, 2008.
- [12] L. B. Oliveira, D. F. Aranha, C. P. Gouvea, M. Scott, D. F. Camara, J. Lopez, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer Communications*, vol. 34, no. 3, p. 485493, 2011.

- [13] J. Lee *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication application," in *Proc. Symp. VLSI Circuits*, Hawaii, USA, June 2004, pp. 176–179.
- [14] T. Xu, J. B. Wendt, and M. Potkonjak, "Secure remote sensing and communication using digital pufs," in *2014 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, Oct 2014, pp. 173–184.
- [15] S. Y. Park, S. Lim, D. Jeong, J. Lee, J. S. Yang, and H. Lee, "Pufsec: Device fingerprint-based security architecture for internet of things," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, May 2017, pp. 1–9.
- [16] C. H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32–62, 2017.
- [17] U. Rhrmair, J. L. 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 *2015 IEEE Symposium on Security and Privacy*, May 2015, pp. 70–85.
- [18] 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 Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 11, pp. 2629–2640, Nov 2015.
- [19] Y. Cao, L. Zhang, C. H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 7, pp. 1143–1147, July 2015.
- [20] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug 2014.
- [21] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 9, pp. 2192–2202, Sept. 2016.
- [22] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of RO PUFs," in *Proc. Hardware-Oriented Security and Trust (HOST)*, Austin, TX, USA, Jun. 2013, pp. 19–24.
- [23] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, June 2007, pp. 9–14.
- [24] T. A. Demassa and Z. Ciccone, *Digital Integrated Circuits*. New York: Wiley, 1996.
- [25] R. Kumar, V. Patil, and S. Kundu, "On design of temperature invariant physically unclonable functions based on ring oscillators," in *Proc. IEEE Computer Society Annual Symp. on VLSI (ISVLSI)*, Amherst, MA, USA, Aug. 2012, pp. 165–170.
- [26] (2017, Oct.) Xilinx Vivado design suite. Xilinx. [Online]. Available: <https://www.xilinx.com/support/download.html>
- [27] J. Tang, R. Karri, and J. Rajendran, "Securing pressure measurements using sensorpufs," in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2016, pp. 1330–1333.
- [28] "VC709 Evaluation Board for the Virtex-7 FPGA User Guide," Aug. 2016, uG887 (v1.5.1). [Online]. Available: https://www.xilinx.com/support/documentation/boards_and_kits/vc709/ug887-vc709-eval-board-v7-fpga.pdf
- [29] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication 800-22*, 2010.