sensors

MDPI

Article

A Compact and Low Power RO PUF with High Resilience to the EM Side-Channel Attack and the SVM Modelling Attack of Wireless Sensor Networks

Yuan Cao [1], Xiaojin Zhao [2,*], Wenbin Ye [2], Qingbang Han [1] and Xiaofang Pan [3]

[1] College of Internet of Things Engineering, Hohai University, Changzhou 213022, China; 20161965@hhu.edu.cn (Y.C.); 20111841@hhu.edu.cn (Q.H.)
[2] College of Electronic Science and Technology, Shenzhen University, Shenzhen 518060, China; yewenbin@szu.edu.cn
[3] College of Information Engineering, Shenzhen University, Shenzhen 518060, China; eexpan@szu.edu.cn
* Correspondence: eexjzhao@szu.edu.cn; Tel.: +86-755-2653-4853

Received: 9 December 2017; Accepted: 20 January 2018; Published: 23 January 2018

Abstract: Authentication is a crucial security service for the wireless sensor networks (WSNs) in versatile domains. The deployment of WSN devices in the untrusted open environment and the resource-constrained nature make the on-chip authentication an open challenge. The strong physical unclonable function (PUF) came in handy as light-weight authentication security primitive. In this paper, we present the first ring oscillator (RO) based strong physical unclonable function (PUF) with high resilience to both the electromagnetic (EM) side-channel attack and the support vector machine (SVM) modelling attack. By employing an RO based PUF architecture with the current starved inverter as the delay cell, the oscillation power is significantly reduced to minimize the emitted EM signal, leading to greatly enhanced immunity to the EM side-channel analysis attack. In addition, featuring superior reconfigurability due to the conspicuously simplified circuitries, the proposed implementation is capable of withstanding the SVM modelling attack by generating and comparing a large number of RO frequency pairs. The reported experimental results validate the prototype of a 9-stage RO PUF fabricated using standard 65 nm complementary-metal-oxide-semiconductor (CMOS) process. Operating at the supply voltage of 1.2 V and the frequency of 100 KHz, the fabricated RO PUF occupies a compact silicon area of 250 μm^2 and consumes a power as low as 5.16 μW per challenge-response pair (CRP). Furthermore, the uniqueness and the worst-case reliability are measured to be 50.17% and 98.30% for the working temperature range of $-40\sim120$ °C and the supply voltage variation of $\pm2\%$, respectively. Thus, the proposed PUF is applicable for the low power, low cost and secure WSN communications.

Keywords: wireless sensor network; strong physical unclonable function; ring oscillator; electromagnetic side-channel attack; support vector machine modelling attack

1. Introduction

Wireless sensor networks (WSNs) are intensely ubiquitous and encompass a broad range of new applications, such as AR/VR, Internet of Things (IoT), and vehicle network [1]. The smart sensors are the tentacles that sense the environmental conditions and communicate the information that is usually security and private critical. It is paramount to assure the integrity of the sensing and protect the collected information from malicious attacks during the data transmission through the untrusted communication channels. However, it is not feasible to implement the conventional cryptography modules on the resource-constrained sensor nodes, including advanced encryption standard (AES), elliptic curve cryptography (ECC) and so on. In light of this, the physical unclonable

function (PUF) as a lightweight security primitive has raised more and more interests in the WSN research community [2,3].

PUF, broadly categorized as "weak PUF" and "strong PUF", is an emerging low-cost on-chip secure primitive [2,4–7]. By converting the inherent uncontrollable and unpredictable variations of the semiconductor manufacturing process to a random digital bit string, a PUF generates a "response" upon a "challenge", namely a challenge-response pair (CRP). Weak PUFs target the application of the key generation [2,4], while strong PUFs are more suitable for the device authentication [8]. The weak PUFs generally have very few CRPs. They can be essentially regarded as a special form of memory, which are resilient to the invasive attacks [8]. The strong PUF, as a disorderd physical system, features complex challenge-response behavior and large challenge-response space. It is almost impossible to physically clone a strong PUF, whose CRPs behave exactly the same as the original one. As a result, the strong PUF is more suitable for the wide range of device authentication applications than its counterpart of weak PUF [9–11]. Among the strong PUF implementations, ring oscillator (RO) PUF is superior due to the following reasons [12]: (1) the frequencies of the ROs in the PUF are irrelevant to the delay introduced by the outputs' routing; (2) the difference of the RO pairs' frequencies can be further increased by extending their oscillation time. However, the feature of public CRPs' accessability for strong PUFs renders them vulnerable to modeling attacks [8]. In addition, Merli's work demonstrates that the electromagnetic (EM) measurements are capable of disclosing both the frequency and the location of each RO, which enables the prediction of the RO PUF's CRPs [12].

To address these security threats, this paper presents the first RO based strong PUF design to resist the EM side-channel attack and the support vector machine (SVM) modelling attack. Compared with the previous implementations, the proposed RO PUF features low power consumption, high area efficiency and improved security performance with high entropy. Specifically, in order to minimize the influence of the emitted EM signal, the RO's delay cell consists of the current starved inverters, which operate at the subthreshold region and significantly reduce the overall power consumption. In addition, each RO used to generate the CRP includes one of the two current starved inverters in each inverter stage, resulting in the exponential increment of the RO number in a given area. Furthermore, the RO PUF architecture employs a linear feedback shift register (LFSR) counter to enhance the system's logical reconfigurability and thwart the SVM modelling attack. The rest of the paper is organized as follows. Section 2 introduces the architecture and operation of proposed RO PUF. Experiments results are presented and discussed in Section 3. Finally, the conclusion is drawn in Section 4.

2. Architecture and Operation of Proposed RO PUF

Figure 1 illustrates the architecture of the proposed 9-stage RO PUF. It basically consists of one LFSR counter, one reconfigurable current starved RO and one bidirectional counter. The key component is the reconfigurable current starved RO. Its oscillation frequency is determined by the delay t_d of its current starved inverter stage. Here t_d is given as:

$$t_d = \frac{C_0 V_{dd}}{i_D} \tag{1}$$

where C_0 is the load capacitance, i_D is the average charging/discharging current and V_{dd} is the power supply voltage. The key component in the proposed RO PUF is the MUX based current starved RO with reconfigurability. The delay cell in the RO is the current starved inverter. As shown in Figure 2, two additional bias transistors are added into the regular inverter to realize the current starved inverter.

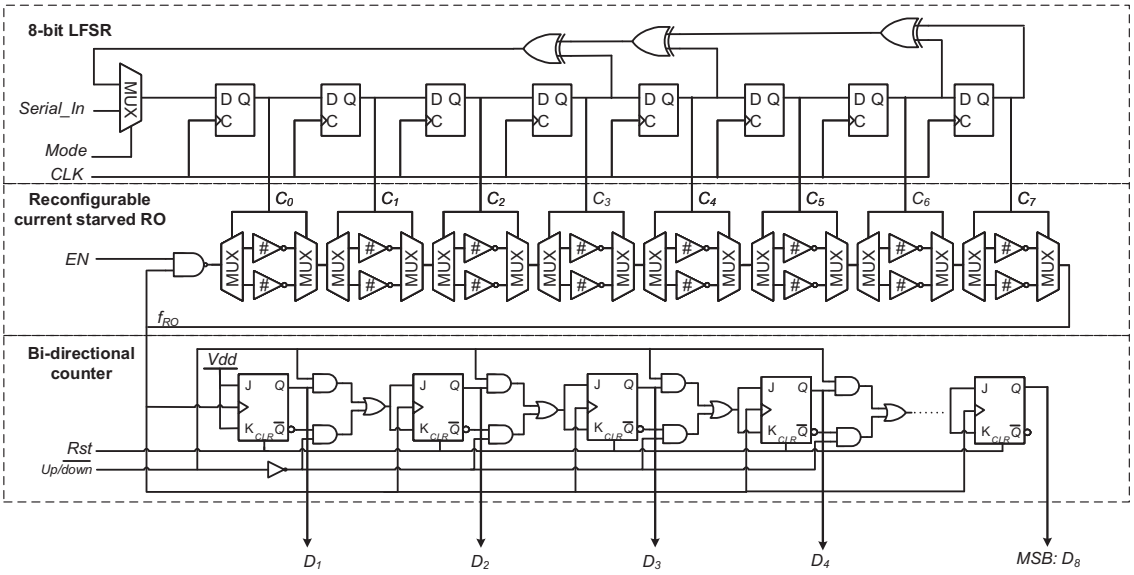

Figure 1. Architecture of the proposed ring oscillator (RO) PUF.

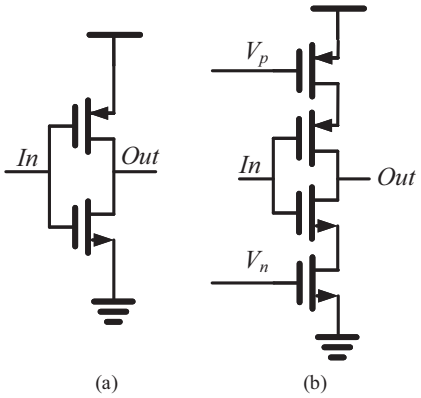

Figure 2. Schematics of (**a**) regular inverter and (**b**) current starved inverter.

In the current starved inverter, the output capacitance is charged/discharged by the maximum drain current I_D of the pull-up/pull-down transistor initially, which is decreased during the transition. Without considering the leakage and short-circuit current, the average current i_D is equal to ηI_D, where the fraction η is fixed for a given device. The current starved inverter can be made to work in the sub-threshold region by biasing the voltages V_p and V_n. The maximum current I_D is formulated by [13]:

$$I_D = \mu C_{OX} \frac{W}{L} (\frac{\kappa_B T}{q})^2 (n-1) e^{\frac{q(V_{GS}-V_t)}{n\kappa_B T}} (1 - e^{-\frac{qV_D}{\kappa_B T}}) \quad (2)$$

$$n = \frac{1 + (C_S + C_{it})}{C_{OX}} \quad (3)$$

where κ_B is the Boltzmann constant; C_S, C_{it} and C_{ox} are the capacitances associated with the semiconductor, fast surface states and gate oxide, respectively. From (2), the current is controlled by the V_{GS} of each transistor. Therefore, the power and oscillation frequency of the RO can be tuned by V_p and V_n. It should be noted that two multiplexors are placed in each inverter stage: one at the gate outputs, the other one at the gate inputs. The multiplexors are realized with transmission gates to reduce their delay and transistor count as shown in Figure 3. It is difficult to model the temperature dependency of the multiplexors as the transistors can operate in several regions [14]. What is more

feasible is to increase their transistors' width to make their contribution to the timing variation of the RO negligible relative to the inverters.

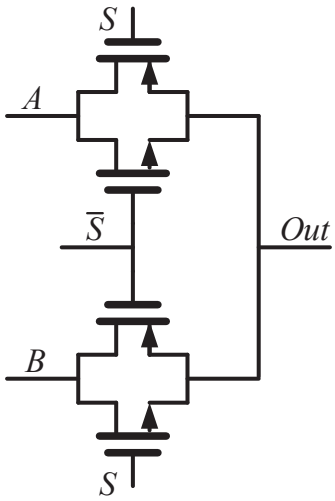

Figure 3. Schematic of the MUX in the proposed physical unclonable function (PUF).

Each response bit of this PUF is produced by comparing two randomly selected ROs' frequencies. The operation of the proposed PUF is explained as follows. The LFSR counter is firstly fed with an 8-bit challenge C through *Serial_In* port by setting the signal *Mode* high. EN in the RO is set to low to disable the oscillation. After C' from the LFSR counter settles down, EN is set to high. Then a rising edge of *Rst* is applied to reset the bidirectional counter, which can record the RO's output frequency. Suppose the RO selected by C is RO_A. Its oscillation frequency f_A is measured by the bidirectional counter with $Up/\overline{down}$ equal to high for a specific time of t. Similarly, another challenge C' is generated by shifting C in the LFSR counter with N_{clk} ($N_{clk} < 2^8$) cycles. The frequency f_B of the new RO RO_B is recorded by the bidirectional counter with $Up/\overline{down}$ set to low for the time of t. Finally, the recorded value in the bidirectional counter represents the frequency difference of the RO pair (i.e. RO_A and RO_B). The most significant bit (MSB) of the bidirectional counter is used as the PUF's output bit. In the proposed RO PUF, the heat generated by the oscillation of RO_A is too small and can be negligible due to the low power feature of the current starved inverter working in the subthreshold region.

It is noted that, with a different N_{clk} in the LFSR counter, the same input challenge can produce different responses for the same PUF instance. As a result, this structure can be considered as a logically reconfigurable PUF [15], In contrast to the controlled PUF (CPUF) [16], which adds simple hash functions to a PUF to forbid the untrusted user to access the PUF directly, the proposed PUF allows for changing the CRP behavior by varying N_{clk}, without the physical replacement and modification of the underlying PUF. This logical reconfigurability makes the proposed PUF more resilient to SVM based attack, which is a subclass of modeling attacks. Modeling attack assumes that the adversary can create a model of the targeted PUF, given a number of CRPs [8]. The rest CRPs can be predicted with the help of this model. To predict the CRPs with SVM, the attackers need to model the CRP generation accurately. Without considering the reconfigurability, N_{clk} for the LFSR counter is assumed to be a known constant. The oscillation frequency of each RO in the proposed PUF is reversely proportional to the sum of the delay in each stage. The applied challenge C/C' selects the top or bottom path.

An additive delay model for the proposed PUF structure can be constructed as follows. The response corresponding to the challenge C can be expressed as:

$$R = \begin{cases} 1 & \text{if} \quad \delta(n+1) > \delta'(n+1) \\ -1 & \text{if} \quad \delta(n+1) < \delta'(n+1) \end{cases} \tag{4}$$

where $\delta(n+1)$ and $\delta'(n+1)$ are the signal delays from the NAND gate input to the output of the RO's last inverter stage (i.e., the $(n+1)$-th) in Figure 1, upon the application of the challenge C and the shadow challenge C' after N_{clk} cycles, respectively. These two delays are then written as:

$$\delta(i) = \frac{1+C_i}{2}p_i + \frac{1-C_i}{2}q_i + \delta(i-1) \tag{5}$$

$$\delta'(i) = \frac{1+C'_i}{2}p_i + \frac{1-C'_i}{2}q_i + \delta'(i-1) \tag{6}$$

where p_i and q_i $(i = 1, 2, \cdots, n+1)$ are the top and bottom inverter delays at the i-th inverter stage of the RO, respectively, and $C_i, C'_i \in \{-1, 1\}$. In contrast to the arbiter PUF whose two competing-signals are generated at the same time (by the rising edge from the very beginning of the delay chain), the proposed RO PUF generates the two competing-signals at different times (one is generated when Challenge C is applied, the other one is generated when the shadow Challenge C' is applied). The frequency distance between two selected ROs is then calculated by subtraction with the help of the following bi-directional counter. Let $\Delta(i)$ denote the difference between $\delta(i)$ and $\delta'(i)$. By subtracting (5) from (6), we can have:

$$\Delta(i) = \frac{p_i - q_i}{2}(C_i - C'_i) + \Delta(i-1) \tag{7}$$

$$\Delta(i) = \frac{p_i - q_i}{2}(C_i - C'_i) + \frac{p_{i-1} - q_{i-1}}{2}(C_{i-1} - C'_{i-1}) \cdots + \Delta(0) \tag{8}$$

where $\Delta(0) = 0$. The final delay difference $\Delta(n+1)$ can be represented as an inner product:

$$\Delta(n+1) = < \overrightarrow{w}, \overrightarrow{x} > \tag{9}$$

where $\overrightarrow{w} = \frac{1}{2}((p_0 - q_0), \cdots, (p_{n+1} - q_{n+1}))$ and $\overrightarrow{x} = ((C_0 - C'_0), \cdots, (C_{n+1} - C'_{n+1}))$. In this way, a separating hyperplane in the space of all feature vectors $\overrightarrow{x}$ can be determined by the SVM. However, if N_{clk} is not fixed but randomly reconfigurable by the user, $\overrightarrow{x}$ becomes unpredictable. In order to secure N_{clk}, N_{clk} can be encrypted and sent along with the challenge to the device when an authentication is inquired.

3. Experimental Results and Discussions

The microphotograph of the fabricated chip using standard 65 nm CMOS process is shown in Figure 4. The proposed PUF's core area is only 5×50 μm^2. The setup of the probe station for the post-silicon test is shown in Figure 5, where *Agilent* oscilloscope with 1GS/s sampling rate is used to measure the output frequencies of the current starved ROs and capture the responses of the PUF. The LFSR counter and other control signals are generated by a *Xilinx Virtex-II Pro* FPGA board externally. Figure 6 shows the distribution of RO's oscillation frequency in one sample chip. There are totally 2^8 = 256 ROs in each PUF instance. The average oscillation frequency is 101 KHz. The most important figures of merits for the PUF, namely, the uniqueness, reliability, power and security are presented and discussed in the following subsections.

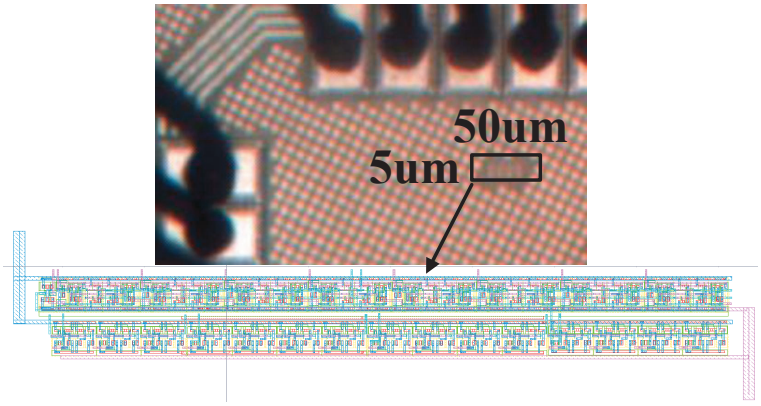

Figure 4. The microphotograph of the proposed RO PUF chip.

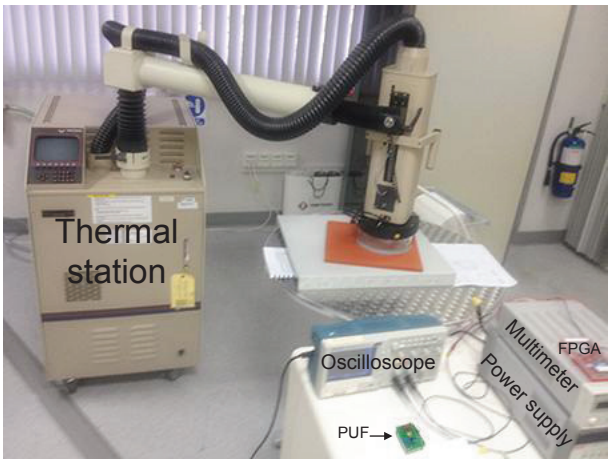

Figure 5. The probe station for testing the sample chips.

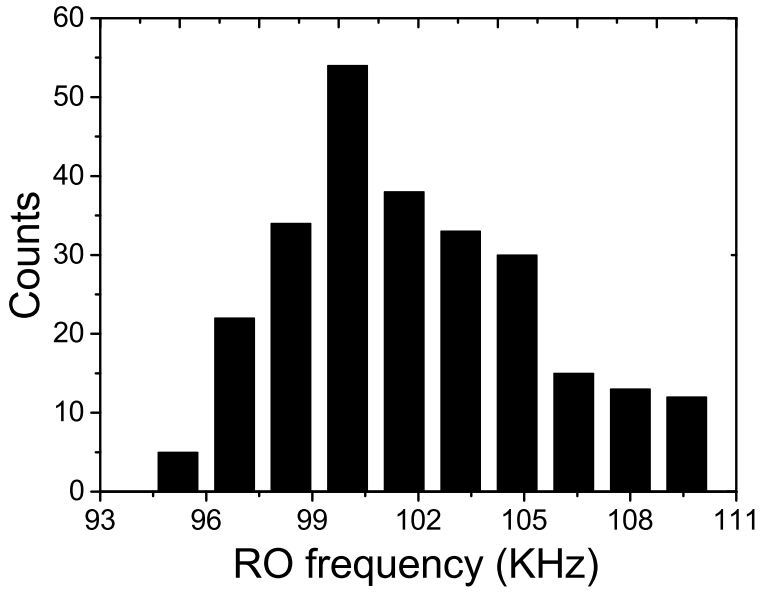

Figure 6. The distribution of RO's oscillation frequency for one sample chip.

3.1. Uniqueness

The uniqueness measures how different the CRPs produced by a PUF are from the other chips. The average inter-die Hamming Distance (HD) of the PUF's CRPs is generally used to calculate the uniqueness. With the same input challenge C to two different chips, u and v, two n-bit responses R_u and R_v can be generated. The average inter-die HD for m chips is expressed as [17]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \tag{10}$$

Figure 7 shows the measured frequency distribution of the inter-die Hamming Distance (HD) for 10 PUF dies. The uniqueness measured from the proposed PUF's inter-die HD is 50.17%, with the ideal value equal to 50%. A Gaussian distribution with mean μ = 50.17% and standard deviation σ = 0.43% can well fit this distribution as shown in Figure 7.

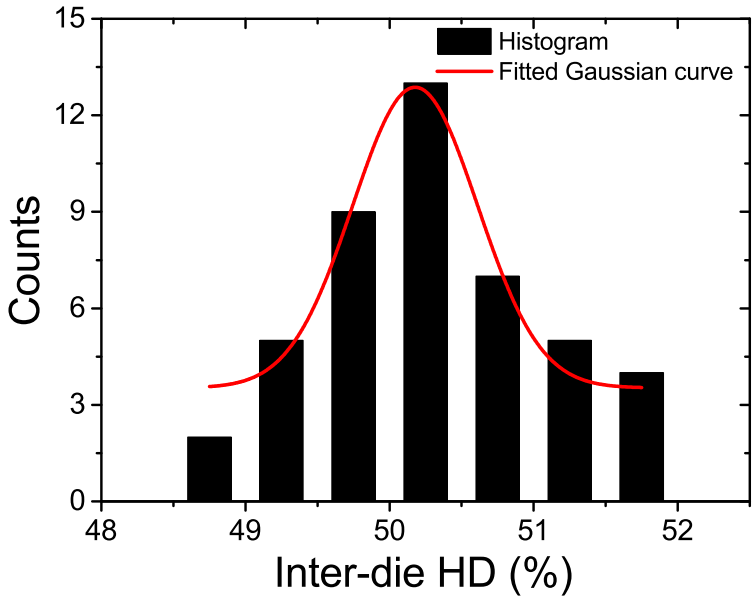

Figure 7. The measured inter-die HD distribution for the proposed RO PUF.

3.2. Reliability

The reliability represents how reproducible the CRPs generated by a PUF are, under variable operating conditions, e.g., different temperature, supply voltage, ambient noises, etc. The intra-die HD is a way to estimate the reliability. Given an input challenge C, each chip i produces an n-bit reference response R_i under the normal operating condition. It is then measured k times with the same set of challenges under varying operation environments. The produced responses are $R_{i,j(j=1,2,\ldots,k)}$. The assessing of reliability for chip i can be written as [17]:

$$S = 1 - BER = 1 - \frac{1}{k} \sum_{j=1}^{k} \frac{HD(R_i, R_{i,j})}{n} \times 100\% \tag{11}$$

where BER stands for the bit error rate. With 1000 CRPs produced by the PUF under various temperatures and supply voltages, the reliability is measured. Figure 8a,b show the fabricated RO PUF's reliability with the temperature and voltage variations, respectively. The worst-case reliability is observed to be 98.30% at −40 °C and 1.22 V. The proposed PUF is characterized with a high temperature reliability over a long temperature range. This is because the delay cell we implemented

in each RO is the current starved inverter. The oscillation frequency of the RO using the current starved inverter is much less sensitive to the temperature variations [18].

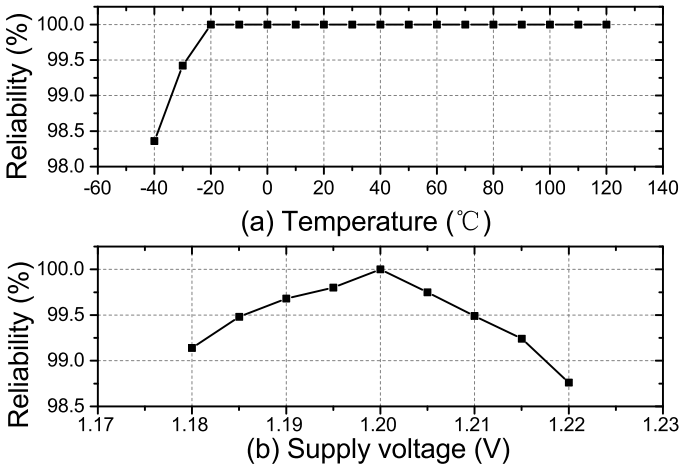

Figure 8. (**a**) The measured average reliability of the proposed RO PUF versus the temperature variations; (**b**) the measured average reliability of the proposed RO PUF versus the voltage variations.

3.3. Power Consumption

In our proposed RO PUF, the RO's frequency and the power consumption can be optimized by tuning V_p and V_n of the current starved inverters. Figure 9 presents the measured average power consumption versus the RO's frequency. It is indicated that the minimum measurable oscillation frequency is 100 KHz and the corresponding power consumption is only 5.16 µW. This low power consumption feature is more suitable for the resource-constrained WSN devices working in the distributed area.

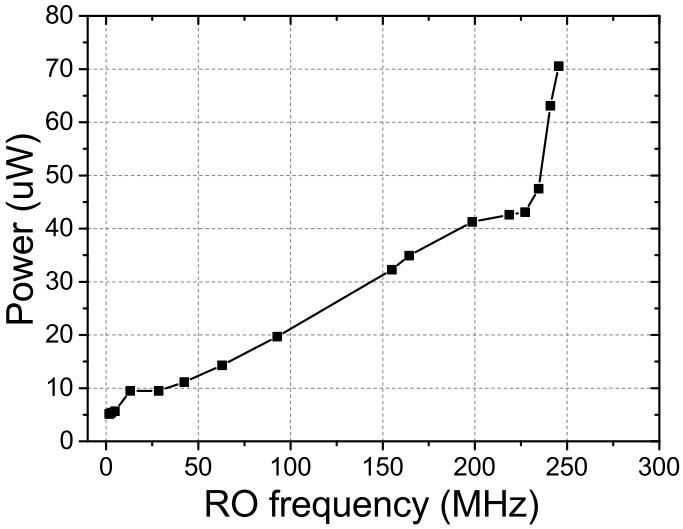

Figure 9. The measured average power consumption per challenge-response pair (CRP) of the proposed PUF at different ROs frequencies.

3.4. Security Analysis

3.4.1. SVM Attack

With the above-mentioned reconfigurability in Section 2, the proposed PUF is able to thwart the SVM modelling attack. In order to have a fair comparison with SVM attack on the 64-stage arbiter [11],

we have extensively simulated a 64-stage proposed PUF using the UMC 65 nm CMOS technology to generate the enough training and testing CRPs. Figure 10 shows the prediction results for the proposed 64-bit RO PUF with and without reconfigurability using the tool SVM^{light} [19]. The reconfigurability is disabled by fixing the value of N_{clk} in the LFSR counter. The prediction accuracy is higher than 90% with only 1000 training CRPs for the RO PUF without reconfigurability. This is because, if the reconfigurable parameter N_{clk} is fixed, the relation of C and C' is fixed. The model for the proposed PUF is similar to the arbiter PUF [11], which is very vulnerable to the SVM attack. However, when the reconfigurability is enabled by setting N_{clk} as a random number, our proposed PUF is proved to be more resilient to the SVM modeling attack, as the SVM predication accuracy for our proposed PUF response only fluctuates around 50% even with a large training set size of ten thousand CRPs.

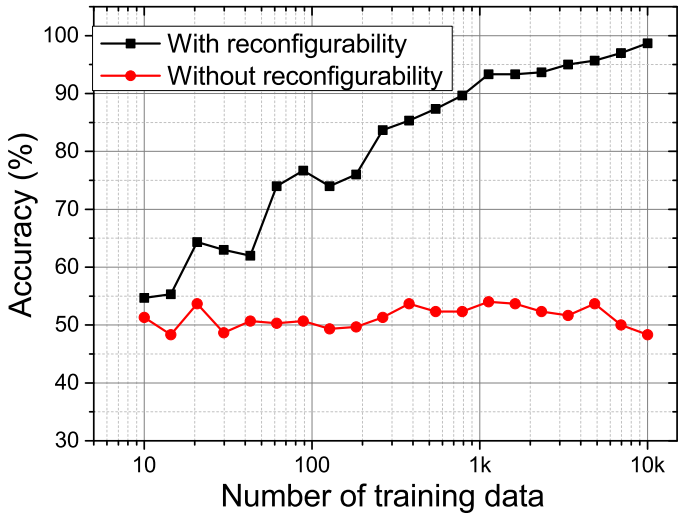

Figure 10. The prediction accuracy by support vector machine (SVM) for the proposed PUF with and without reconfigurability.

3.4.2. EM Side-Channel Attack

EM side-channel attack has been successfully adopted to break the RO PUFs [12]. The analysis is based on the study and comparison of the detectable EM emanations' frequency spectrum for the active RO. According to Friis transmission equation [20]:

$$P_r = G_t G_r (\frac{\lambda}{4\pi R})^2 P_t \tag{12}$$

where G_t and G_r are the antenna gains of the transmitting and receiving antennas, respectively, λ is the wavelength, R is the distance from the detector probe to the device, P_r is detectable magnitude of the EM radiation and P_t is the device's working power consumption. Our proposed hybrid RO PUF has lower power consumption over the classic RO PUF. Since P_r is proportional to P_t, it will have a lower magnitude of EM radiation.

To validate our proposed PUF's resilience against EM side-channel attack, *FLS 106* IC scanner is used to capture the EM radiation close to the fabricated chip's surface. Figure 11a,b illustrate the measured spectrum of the regular RO and the proposed RO fabricated in the same chip, respectively. It is noticed that an EM radiation of 100.38 dBµV at 278 MHz is detected for the regular RO, however, the EM radiation magnitude of the proposed RO is too small to be distinguished from the noise floor. Additionally, as the proposed RO PUF only occupies a tiny silicon area with an interleaving structure, it is quite challenging to pinpoint it on the chip, which further elevated the proposed RO's security performance [21].

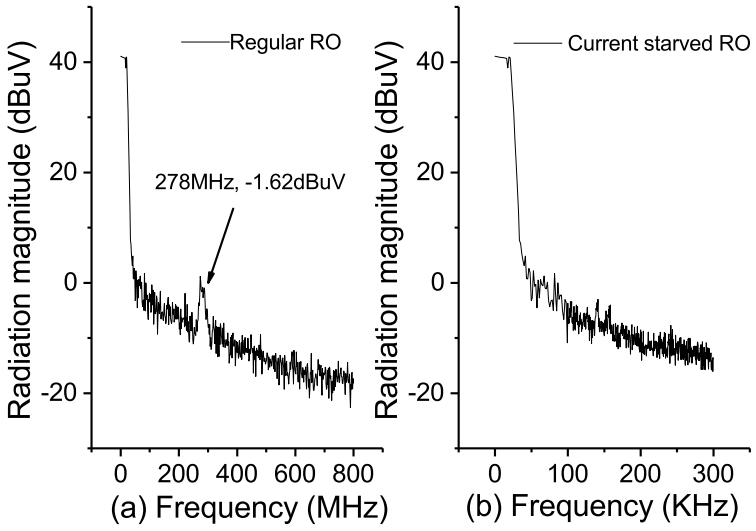

Figure 11. (**a**) The measured EM radiation for the regular RO; (**b**) the measured EM radiation for the proposed RO.

4. Conclusions

In this paper, we present a compact RO PUF with high resilience to both the EM side-channel attack and the SVM modelling attack. By utilizing the current starved inverters as the RO's delay cell, both the oscillation power and the emitted EM signal are minimized, leading to significantly enhanced immunity to the EM based side-channel attack. Additionally, the prototype of the proposed PUF fabricated using 65 nm CMOS process only consumes a low power of 5.16 μW per CRP at 1.2 V, under an oscillation frequency of 100 KHz. In addition, the measured CRPs exhibits a superior uniqueness of 50.17% and a BER of 1.7% with the operation temperature varied from −40 °C to 120 °C. Furthermore, with the external challenge randomized by the incorporated LFSR counter, the reconfigurable CRPs are capable of providing substantial resilience to the prediction attack by SVM. The proposed PUF shows great promise to a wide range of light-weight WSN security applications with limited battery capacity.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (Grant No. 61601168, 61504087, 11574072), the Fundamental Research Funds for the Central Universities (Grant No. 2016B15314), the Key Research Project of Jiangsu Province (Grant No. BE2016056) and the Fundamental Research Foundation of Shenzhen (Grant No. JCYJ20170302151209762 and JCYJ20160520170741660).

Author Contributions: All authors have contributed to this work. Yuan Cao proposed the VLSI architecture, conducted the simulation and drafted the manuscript. Xiaojin Zhao and Qingbang Han conducted the theoretical deduction. Wenbin Ye and Xiaofang Pan analyzed the experimental results. All authors have read and revised the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ergen, S.C.; Sangiovanni-Vincentelli, A. Intravehicular energy-harvesting wireless networks: Reducing costs and emissions. *IEEE Veh. Technol. Mag.* **2017**, *12*, 77–85.
2. Liu, R.; Wu, H.; Pang, Y.; Qian, H.; Yu, S. Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays. *IEEE Electron Device Lett.* **2015**, *36*, 1380–1383.
3. Li, D.; Lu, Z.; Zou, X.; Liu, Z. PUFKEY: A high-security and high-throughput hardware true random number generator for sensor networks. *Sensors* **2015**, *15*, 26251–26266.
4. Kim, M.S.; Moon, D.I.; Yoo, S.K.; Lee, S.H.; Choi, Y.K. Investigation of physically unclonable functions using flash memory for integrated circuit authentication. *IEEE Trans. Nanotechnol.* **2015**, *14*, 384–389.
5. Das, J.; Scott, K.; Rajaram, S.; Burgett, D.; Bhanja, S. MRAM PUF: A novel geometry based magnetic PUF with integrated CMOS. *IEEE Trans. Nanotechnol.* **2015**, *14*, 436–443.

6. Chen, A. Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions. *IEEE Electron Device Lett.* **2015**, *36*, 138–140.
7. Li, J.; Seok, M. Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators. *IEEE J. Solid-State Circuits* **2016**, *51*, 2192–2202.
8. Rührmair, U.; Sölter, J.; Sehnke, F.; Xu, X.; Mahmoud, A.; Stoyanova, V.; Dror, G.; Schmidhuber, J.; Burleson, W.; Devadas, S. PUF modeling attacks on simulated and silicon data. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1876–1891.
9. Yang, K.; Dong, Q.; Blaauw, D.; Sylvester, D. A physically unclonable function with BER $< 10^{-8}$ for robust chip authentication using oscillator collapse in 40 nm CMOS. In Proceedings of the 2015 IEEE International Solid State Circuits Conference, San Francisco, CA, USA, 22–26 February 2015; pp. 1–3.
10. Komurcu, G.; Pusane, A.; Dundar, G. Analysis of ring oscillator structures to develop a design methodology for RO-PUF circuits. In Proceedings of the International Conference on Very Large Scale Integration (VLSI-SoC), Istanbul, Turkey, 7–9 October 2013; pp. 332–335.
11. Lin, L.; Srivathsa, S.; Krishnappa, D.K.; Shabadi, P.; Burleson, W. Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1394–1403.
12. Merli, D.; Heyszl, J.; Heinz, B.; Schuster, D.; Stumpf, F.; Sigl, G. Localized electromagnetic analysis of RO PUFs. In Proceedings of the Hardware-Oriented Security and Trust (HOST), Austin, TX, USA, 2–3 June 2013; pp. 19–24.
13. Taur, Y.; Ning, T. *Fundamentals of Modern VLSI Devices*; Cambridge University Press: Cambridge, UK, 1998.
14. Mondal, S.; Talapatra, S.; Rahaman, H. Analysis, modeling and optimization of transmission gate delay. In Proceedings of the Asia Symposium on Quality Electronic Design (ASQED), Kuala Lumpur, Malaysia, 19–20 July 2011; pp. 246–253.
15. Katzenbeisser, S.; Koçabas, Ü.; Van Der Leest, V.; Sadeghi, A.R.; Schrijen, G.J.; Schröder, H.; Wachsmann, C. Recyclable PUFs: Logically reconfigurable PUFs. *J. Cryptogr. Eng.* **2011**, *1*, 177–186.
16. Gassend, B.; Clarke, D.; Van Dijk, M.; Devadas, S. Silicon physical random functions. In Proceedings of the ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp. 148–160.
17. Maiti, A.; Schaumont, P. Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators. In Proceedings of the International Conference on Field Programmable Logic and Applications, Prague, Czech Republic, 31 August–2 September 2009; pp. 703–707.
18. Ramazani, A.; Biabani, S.; Hadidi, G. CMOS ring oscillator with combined delay stages. *Int. J. Electron. Commun.* **2014**, *68*, 515–519.
19. Joachims, T. Learning to classify text using support vector machines: Methods, theory and algorithms. *Comput. Linguist.* **2003**, *29*, 655–664.
20. Hogg, D. Fun with the Friis free-space transmission formula. *IEEE Antennas Propag. Mag.* **1993**, *35*, 33–35.
21. He, W.; de la Torre, E.; Riesgo, T. An interleaved EPE-immune PA-DPL structure for resisting concentrated EM side channel attacks on FPGA implementation. In Proceedings of the International Conference on Constructive Side-Channel Analysis and Secure Design (COSADE), Darmstadt, Germany, 3–4 May 2012; pp. 39–53.

© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).