engineering proceedings

MDPI

Proceeding Paper

A Ring Oscillator-Based Physical Unclonable Function with Enhanced Challenge–Response Pairs to Improve the Security of Internet of Things Devices †

Marco Grossi *, Martin Omaña, Cecilia Metra and Andrea Acquaviva

Department of Electrical Energy and Information Engineering "Guglielmo Marconi" (DEI), University of Bologna, 40136 Bologna, Italy; martin.omana@unibo.it (M.O.); cecilia.metra@unibo.it (C.M.); andrea.acquaviva@unibo.it (A.A.)

* Correspondence: marco.grossi8@unibo.it; Tel.: +39-0512093038

† Presented at the 11th International Electronic Conference on Sensors and Applications (ECSA-11), 26–28 November 2024; Available online: https://sciforum.net/event/ecsa-11.

Abstract: Portable and wearable sensor systems implemented in the paradigm of the Internet of Things (IoT) are part of our daily activities as well as commercial and industrial products. The connection of measurement devices has led to not only a sharp increase in information sharing, but also to the frequency of cyber-attacks, in which system vulnerabilities are exploited to steal confidential information, corrupt data, or even make the system unavailable. Physical unclonable function (PUF)-based devices exploit the inherent randomness introduced during device manufacturing to create a unique fingerprint. They are widely used to generate passwords and cryptographic keys to mitigate security issues in IoT applications. Among the existing different PUF structures, ring oscillator (RO)-based PUF devices are very popular due to their simple structure and their potential easy integration onto chips. In this paper, the possibility of increasing the number of challenge–response pairs (CRPs) of RO-based PUF devices by measuring two different parameters (the oscillation frequency and the duty cycle) is investigated. The results achieved by the performed circuit level simulations and experimental measurements show that these two parameters feature a weak correlation. The proposed PUF device can be used to increase the number of CRPs to improve device security while achieving a high uniqueness value (49.77%).

Keywords: physical unclonable function; ring oscillator; frequency; duty cycle; cybersecurity; internet of things

Citation: Grossi, M.; Omaña, M.; Metra, C.; Acquaviva, A. A Ring Oscillator-Based Physical Unclonable Function with Enhanced Challenge–Response Pairs to Improve the Security of Internet of Things Devices. *Eng. Proc.* **2024**, *82*, 15. https://doi.org/10.3390/ecsa-11-20497

Academic Editor: Stefan Bosse

Published: 26 November 2024

1. Introduction

Portable sensor systems are part of our daily activities as well as commercial and industrial products, mainly due to their ability to perform measurements in-the-field by non-trained personnel. These sensor systems are adopted in different application fields, such as environmental monitoring [1,2], food quality analysis [3–5], smart home automation [6,7], microbiological measurements [8,9], and quality control in Industry 4.0 [10,11]. Many sensor systems are designed considering the paradigm of the Internet of Things (IoT), in which measured data are exchanged with remote servers by wireless communication. The connection of sensor nodes, however, implies significant security risks, since unauthorized entities may exploit system vulnerabilities to steal confidential information, corrupt data, or even to make the system unavailable [12].

Different countermeasures have been proposed to mitigate the risks related to cyber-attacks and to increase system security [13–15]. For example, authentication procedures can be used to prevent unauthorized access to systems [16], while cryptography can be adopted to obfuscate confidential data, making information useless for any malicious user listening

to the communication [17]. Even if these techniques are very effective in mitigating cyber-attacks, passwords for authentication procedures and keys for cryptographic algorithms are usually stored in non-volatile memory. Therefore, hacking such non-volatile memory results in the disclosure of confidential information, producing a security breach.

An alternative solution to the storage of authentication passwords and cryptographic keys on non-volatile memory is represented by physical unclonable function (PUF) devices, which exploit the inherent randomness introduced during manufacturing to produce a unique device response to a given input [18]. Different architectures for PUF devices have been proposed, such as Arbiter PUFs [19], ring oscillator (RO) PUFs [20], and static RAM-based PUFs [21]. RO PUFs are, in particular, very popular since the RO is a simple circuit and does not require high symmetry; thus, they are very attractive for on-chip integration. However, RO PUFs consume more resources than other PUF architectures, while also generating a limited number of challenge–response pairs (CRPs) [22].

While standard RO-based PUF devices generate responses by comparing the oscillation frequency of RO circuits, alternative solutions have been proposed in the literature. For example, in 2018, Azhar et al. presented a duty cycle-based RO PUF device [23]. The authors showed that, in an RO circuit, the standard deviation of the duty cycle distribution decreases less than the standard deviation of the oscillation frequency distribution as the number of RO-inverting stages increases, thus producing a more secure PUF device. However, the number of CRPs achieved using the proposed approach remains the same as that of the standard RO PUF device.

In this paper, an alternative RO PUF approach is proposed, which features an increased number of CRPs. The proposed approach is based on the measurement of two different parameters for each RO circuit, namely the oscillation frequency and the duty cycle. The results of circuit-level simulations and experimental measurements show that these two parameters feature a low correlation, and thus they can be used to increase the PUF response size for a fixed number of RO circuits while achieving a high value of uniqueness (49.77%). In Section 2, the working principle of the proposed RO PUF approach to increase the number of CRPs is presented. In Section 3, the correlation between the oscillation frequency and the duty cycle of the output signal of an RO circuit is investigated by means of Monte Carlo simulations. In Section 4, the correlation between the oscillation frequency and the duty cycle of the output signal of an RO circuit is analyzed by means of experimental measurements of RO circuits implemented by discrete components on a breadboard. Finally, conclusive remarks are presented in Section 5.

2. Proposed PUF Implementation

The structure of an RO circuit implemented by CMOS technology is shown in Figure 1. It consists of a NAND gate with its output driving a chain of an even number of NOT gates (NOT_1, NOT_2, ……, NOT_n). The output X_n of the last NOT gate in the chain is feedbacked into one input of the NAND gate, while the other input of the NAND gate is the signal EN, used to enable/disable the RO circuit. The last NOT gate of the circuit (NOT_{buffer}) is an output buffer used to drive the next stage circuit.

The implementation of the proposed RO PUF approach is schematically represented in Figure 2. It consists of N different copies of the RO circuit (RO_1, RO_2, ……, RO_N), whose outputs are connected to the inputs of two multiplexers (MUX_1 and MUX_2). When two different RO circuits (for example, RO_i and RO_j) are selected by means of the input challenge, the outputs of RO_i and RO_j are provided at the output of the two multiplexers (OUT_1 and OUT_2, respectively) and are used to generate the 2-bit PUF response (RB_{fosc}, RB_{DC}).

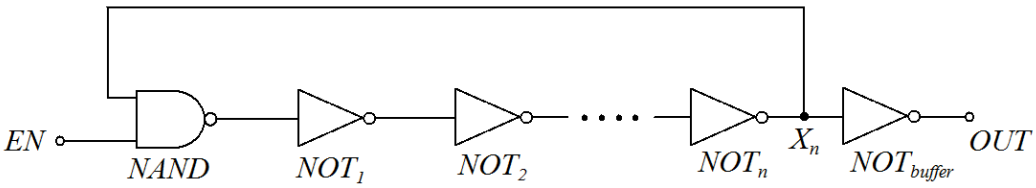

Figure 1. The structure of a ring oscillator circuit in CMOS technology.

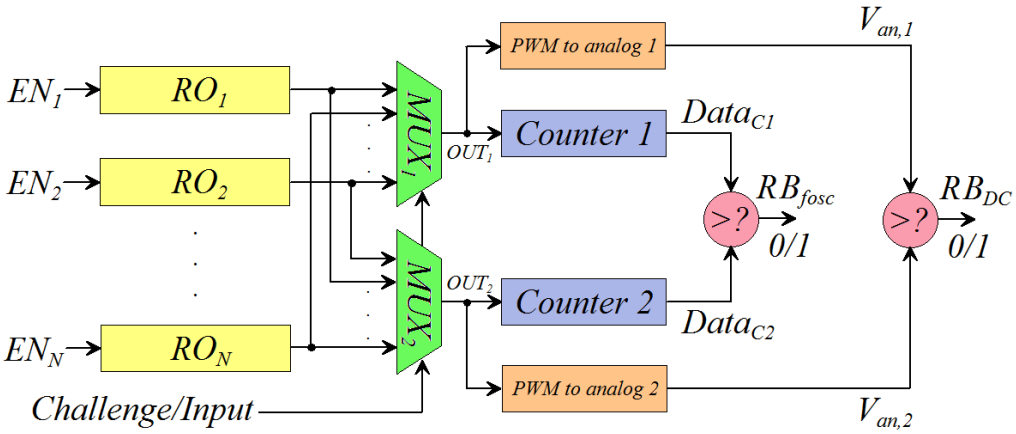

Figure 2. The implementation of the proposed ring oscillator PUF approach.

The response bit RB_{fosc} is generated as follows:

1. Signals OUT_1 and OUT_2 are used as clocks for the two counters, Counter 1 and Counter 2.
2. The two counters are initially reset and then enabled for a fixed period of time.
3. After the counting time period expires, the outputs of the two counters are proportional to the oscillation frequencies of the two selected ROs, that is, $Data_{C1}$ is proportional to $f_{osc,ROi}$ and $Data_{C2}$ is proportional to $f_{osc,ROj}$. Thus, RB_{fosc} equals 1, if $Data_{C1} > Data_{C2}$, and 0 otherwise.

The response bit RB_{DC} is generated as follows:

1. Signals OUT_1 and OUT_2 are provided as inputs to the two circuits 'PWM to analog 1' and 'PWM to analog 2'.
2. The circuit 'PWM to analog 1' generates an analog voltage $V_{an,1}$ that is proportional to the duty cycle of the square-wave signal OUT_1. Similarly, $V_{an,2}$ is proportional to the duty cycle of the square-wave signal OUT_2.
3. An analog comparator generates RB_{DC} equal to 1, if $V_{an,1} > V_{an,2}$, and 0 otherwise.

In the case of N RO circuits, the number of possible comparisons among couples of RO circuits is $C_{N,2} = \frac{N(N-1)}{2}$. Since a single RO circuit out of N can be addressed by $\lceil log_2 N \rceil$ bits, the couple of ROs can be selected by $2 \cdot \lceil log_2 N \rceil$ bits, while the challenge length to select k different couples of RO circuits is $2 \cdot \lceil log_2 N \rceil \cdot k$ bits.

The standard RO PUF approach generates a single response bit for each couple of selected ROs. Thus, the selection of k different couples of ROs generates a k-bit PUF response.

In the proposed RO PUF approach, instead, by measuring both the oscillation frequency and the duty cycle, we enable the generation of a 2-bit response for each couple of RO circuits. Thus, by selecting k different couples of RO, we generate a 2 k-bit PUF response. This results in an increase in the number of CRPs for the same number of ROs or, alternatively, in the generation of the same number of CRPs using a lower number of ROs, with advantages in terms of the area overhead. However, to guarantee high levels of security, the two measured parameters (oscillation frequency and duty cycle) must be uncorrelated. Otherwise, a strong correlation between such two parameters would

result in the decreased uniqueness of the generated response, with a negative impact on PUF security.

3. Results Achieved by Circuit Level Simulations

The RO circuit presented in Figure 1 was simulated using LTSpice (Analog devices, Norwood, MA, USA), considering its implementation by a standard 180 nm CMOS technology [24]. The RO circuit was designed considering n = 4 NOT gates in the inverters chain, and a power supply of V_{DD} = 3.3V. The device sizes were L = W = 180 nm for the NMOS transistors, and L = 180 nm and W = 360 nm for the PMOS transistors. A capacitance of 100 pF was connected between the output of each logic gate (NAND and NOT) and the ground. A Monte Carlo analysis was performed considering a Gaussian distribution for the transistors' oxide thickness (T_{ox}), channel mobility (U_0), and threshold voltage (V_{th}), with a 10% tolerance. The obtained average value μ, and standard deviation σ of such parameters are presented in Table 1. The Monte Carlo analysis consisted of 256 steps to simulate a PUF device featuring 256 ROs of the type presented in Figure 1. For each RO (RO_i, i = 0…255) the oscillation frequency $f_{osc,i}$ and the duty cycle DC_i were calculated.

Table 1. The average value (μ) and standard deviation (σ) for the distribution of oxide thickness (T_{ox}), channel mobility (U_0), and transistor threshold voltage (V_{th}) generated with the performed Monte Carlo simulations.

	T_{ox} (nm)		U_0 ($cm^2/(V \cdot s)$)		V_{th} (mV)	
	μ	σ	μ	σ	μ	σ
NMOS	4.11	0.13	273.25	9.35	366.98	10.91
PMOS	4.10	0.13	115.29	3.58	−390.17	13.64

The set of 256 values of oscillation frequency follows a Gaussian distribution with a $f_{osc,min}$ = 137.94 kHz, a $f_{osc,max}$ = 151.33 kHz, an average value of 143.65 kHz, and a standard deviation of 2.19 kHz. The set of 256 values of the duty cycle, instead, follows a Gaussian distribution with DC_{min} = 41.49%, DC_{max} = 43.56%, an average value of 42.58%, and a standard deviation of 0.31%. Figure 3 presents the scatter plot showing the duty cycle variation with respect to the oscillation frequency of each RO. As can be seen, the two variables feature a weak correlation, with a coefficient of determination R^2 = 0.098.

For each one of the $C_{256,2}$ = 32640 possible comparisons between a couple of ROs, the PUF response bit was calculated for the oscillation frequency (RB_{fosc}) and the duty cycle (RB_{DC}), as presented in Section 2. A contingency table that displays the number of occurrences as a function of RB_{fosc} and RB_{DC} was calculated and a chi-squared test was carried out to evaluate the correlation between the PUF RB_{fosc} and RB_{DC}. Figure 4 shows a 3D view of the contingency table, in which the number of outcomes (out of all the possible 32640 ones) are plotted with respect to the PUF response bit for the oscillation frequency and duty cycle. The correlation between RB_{fosc} and RB_{DC} was evaluated with the Pearson Phi coefficient (φ) [25]. The values of φ are in the range -1 to +1, where values of ±1 indicate a strong correlation between the variables, while a value of 0 indicates the absence of correlation. The obtained value of φ was 0.184, thus indicating a weak correlation between RB_{fosc} and RB_{DC}.

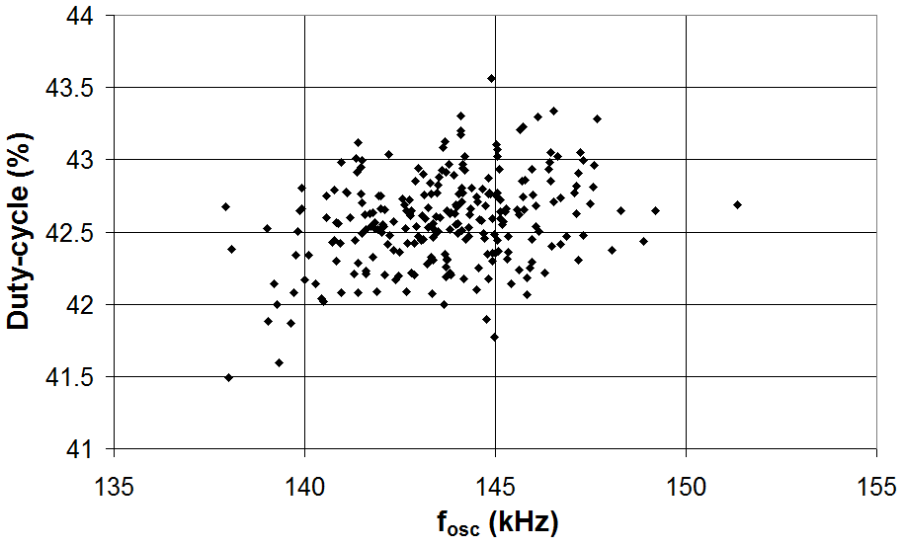

Figure 3. A scatter plot of the duty cycle vs. the oscillation frequency for each RO obtained by Monte Carlo simulations.

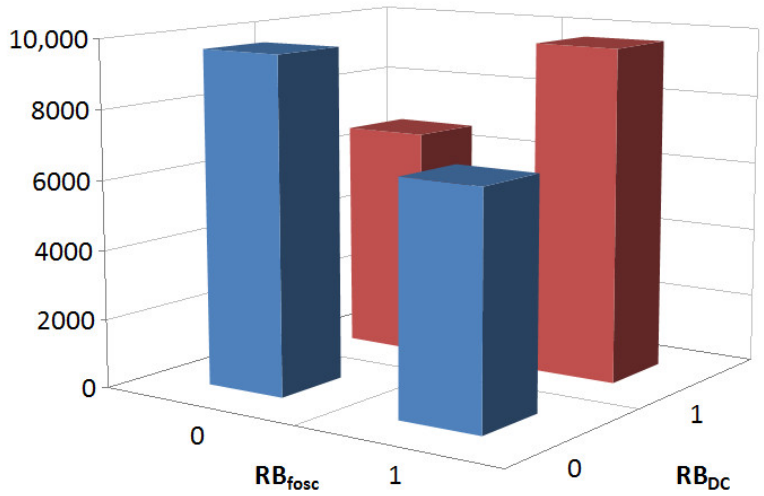

Figure 4. A 3D view of the contingency table of the PUF responses RB_{fosc} and RB_{DC} obtained with Monte Carlo simulations.

As known, the uniqueness figure of metric, as defined in [26], is normally used to evaluate the difference in the response of two different PUF devices to the same challenge. Its optimum value is 50%. The uniqueness was calculated for both the standard RO PUF device and the proposed RO PUF device, in the case of five different PUF devices with a 128-bit response and 10,000 different CRPs. The achieved results show that the uniqueness of the proposed RO PUF approach is 49.77%. Therefore, it is very close to the optimum value and closer than that of a standard RO PUF device (which is equal to 51.01%).

4. Results Achieved by Experimental Measurements

We also performed experimental measurements of the RO circuit presented in Figure 1. We used the SN74HC00N (Texas Instruments, Dallas, TX, USA) commercial integrated circuit. It was implemented with 180nm CMOS technology and featured four 2-input NAND logic gates [27]. The RO circuit was created on a breadboard with fly wires using two SN74HC00N chips. Different replicas of the RO circuit (45) were implemented using the combination of ten different SN74HC00N chips. For each RO circuit, we measured the oscillation frequency f_{osc} and the duty cycle by using the built-in measurement tool of a

TDS 2012B digital oscilloscope (Tektronix, Beaverton, OR, USA) [28]. The measurement setup is presented in Figure 5.

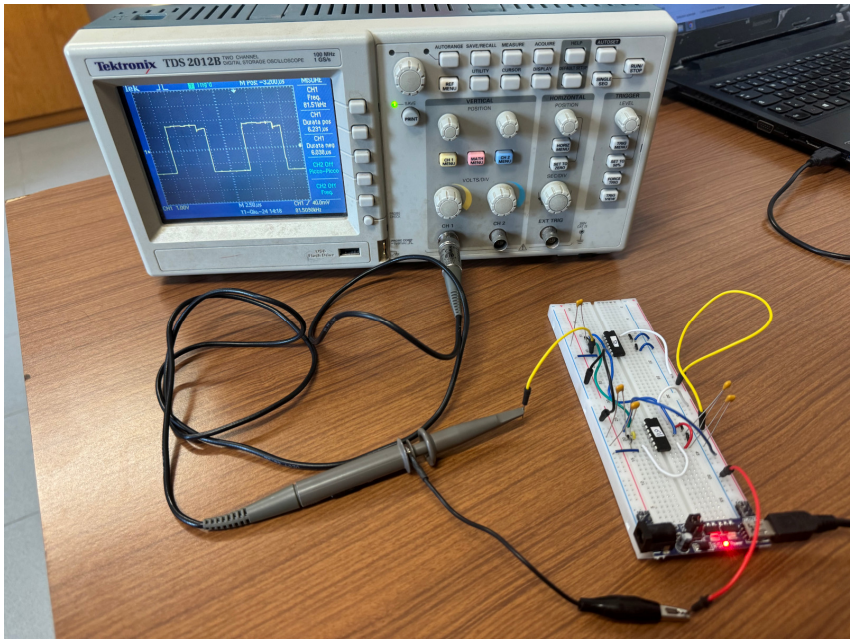

Figure 5. The experimental setup for the measurements on the RO-based PUF device implemented using the SN74HC00N integrated circuit.

The set of 45 values of the oscillation frequency follows a Gaussian distribution with $f_{osc,min}$ = 81.55 kHz, $f_{osc,max}$ = 88.78 kHz, an average value of 84.42 kHz, and a standard deviation of 1.87 kHz. The set of 45 values of the duty cycle instead follows a Gaussian distribution with DC_{min} = 50.79%, DC_{max} = 51.5%, an average value of 51.08%, and a standard deviation of 0.2%. Figure 6 shows the scatter plot of duty cycle variations with respect to the oscillation frequency for each RO. As can be seen, the two considered variables present a weak correlation with a coefficient of determination of R^2 = 0.1123.

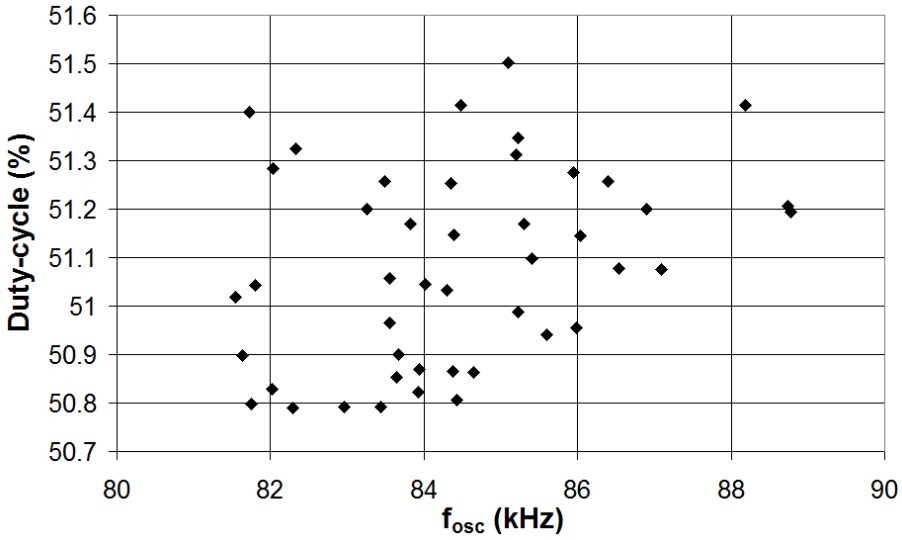

Figure 6. A scatter plot of the duty cycle vs the oscillation frequency for each RO obtained by experimental measurements.

For each of the $C_{45,2}$ = 990 possible comparisons between a couple of ROs, the PUF response bit was calculated for the oscillation frequency (RB_{fosc}) and the duty cycle (RB_{DC}).

A contingency table was calculated and a chi-squared test was performed to evaluate the correlation between the PUF RB_{fosc} and RB_{DC}. Figure 7 reports a 3D view of the contingency table, in which the number of outcomes (out of all possible 990 ones) are plotted with respect to the PUF response bit for the oscillation frequency and the duty cycle. The obtained value of the Pearson Phi coefficient φ is 0.225, thus showing a weak correlation between RB_{fosc} and RB_{DC}.

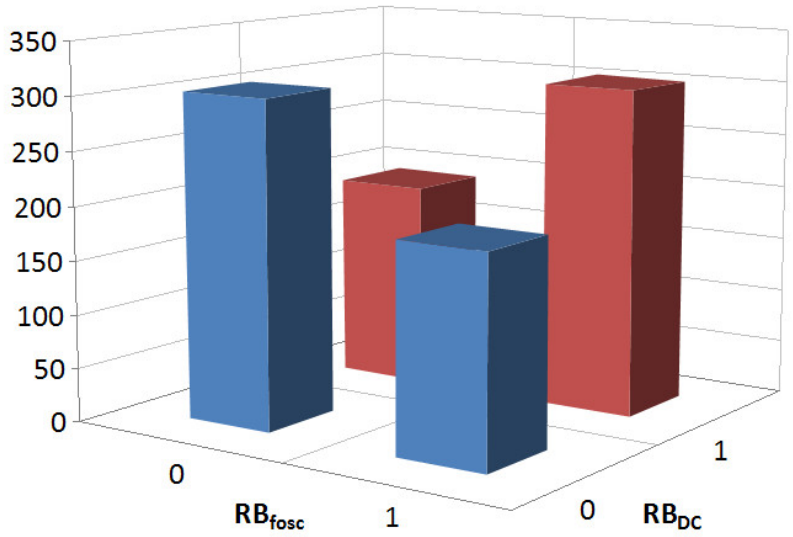

Figure 7. A 3D view of the contingency table of the PUF responses RB_{fosc} and RB_{DC} obtained by experimental measurements.

Overall, the experimental measurements confirmed the results achieved by the performed circuit level simulations. The weak correlation between the oscillation frequency and the duty cycle of the RO circuit allowed us to implement RO-based PUF devices with a response based on both the oscillation frequency and the duty cycle. This allowed us to obtain a 2-bit response for each couple of ROs, thus increasing the number of PUF CRPs and therefore the device security.

5. Conclusions

In this paper, a novel RO-based PUF approach was proposed which generates a response by the measurement of both the oscillation frequency and the duty cycle of the RO circuits. The results of the performed circuit-level simulations and experimental measurements show that the two parameters (the oscillation frequency and the duty cycle) feature a weak correlation and, therefore, can be used to generate the PUF response without decreasing device uniqueness. The proposed implementation allows us to double the number of response bits for a fixed number of ROs while achieving a high value for uniqueness (49.77%). Thus, the number of PUF CRPs can be increased, with benefits in terms of higher device security.

Author Contributions: Conceptualization, M.G.; methodology, M.G.; software, M.G.; validation, M.G.; formal analysis, M.G. and M.O.; investigation, M.G. and M.O.; resources, M.G.; data curation, M.G.; writing—original draft preparation, M.G.; writing—review and editing, M.G. and M.O.; supervision, C.M. and A.A.; project administration, C.M. and A.A.; funding acquisition, C.M. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union—NextGenerationEU under the National Recovery and Resilience Plan (PNRR)—Mission 4 Education and research—Component 2 From research to business—Investment 1.3, Notice D.D. 341 of 15/03/2022, from title: SEcurity and RIghts in the CyberSpace, proposal code PE0000014—CUP J33C22002810001.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

References

1. Spinelle, L.; Gerboles, M.; Kok, G.; Persijn, S.; Sauerwald, T. Review of portable and low-cost sensors for the ambient air monitoring of benzene and other volatile organic compounds. *Sensors* **2017**, *17*, 1520. [CrossRef] [PubMed]
2. Ziętek, B.; Banasiewicz, A.; Zimroz, R.; Szrek, J.; Gola, S. A portable environmental data-monitoring system for air hazard evaluation in deep underground mines. *Energies* **2020**, *13*, 6331. [CrossRef]
3. Grossi, M.; Bendini, A.; Valli, E.; Gallina Toschi, T. Field-Deployable Determinations of Peroxide Index and Total Phenolic Content in Olive Oil Using a Promising Portable Sensor System. *Sensors* **2023**, *23*, 5002. [CrossRef]
4. Grossi, M.; Valli, E.; Bendini, A.; Gallina Toschi, T.; Riccò, B. A Portable Battery-Operated Sensor System for Simple and Rapid Assessment of Virgin Olive Oil Quality Grade. *Chemosensors* **2022**, *10*, 102. [CrossRef]
5. Popa, A.; Hnatiuc, M.; Paun, M.; Geman, O.; Hemanth, D.J.; Dorcea, D.; Hoang Son, L.; Ghita, S. An intelligent IoT-based food quality monitoring approach using low-cost sensors. *Symmetry* **2019**, *11*, 374. [CrossRef]
6. Al-Kuwari, M.; Ramadan, A.; Ismael, Y.; Al-Sughair, L.; Gastli, A.; Benammar, M. Smart-home automation using IoT-based sensing and monitoring platform. In Proceedings of the IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG), Doha, Qatar, 10–12 April 2018; pp. 1–6.
7. Jabbar, W.A.; Kian, T.K.; Ramli, R.M.; Zubir, S.N.; Zamrizaman, N.S.; Balfaqih, M.; Shepelev, V.; Alharbi, S. Design and fabrication of smart home with internet of things enabled automation system. *IEEE Access* **2019**, *7*, 144059–144074. [CrossRef]
8. Grossi, M.; Parolin, C.; Vitali, B.; Riccò, B. Computer vision approach for the determination of microbial concentration and growth kinetics using a low cost sensor system. *Sensors* **2019**, *19*, 5367. [CrossRef]
9. Grossi, M.; Parolin, C.; Vitali, B.; Riccò, B. Measurement of bacterial concentration using a portable sensor system with a combined electrical-optical approach. *IEEE Sens. J.* **2019**, *19*, 10693–10700. [CrossRef]
10. Hinojosa-Meza, R.; Olvera-Gonzalez, E.; Escalante-Garcia, N.; Dena-Aguilar, J.A.; Montes Rivera, M.; Vacas-Jacques, P. Cost-Effective and Portable Instrumentation to Enable Accurate pH Measurements for Global Industry 4.0 and Vertical Farming Applications. *Appl. Sci.* **2022**, *12*, 7038. [CrossRef]
11. Grossi, M.; Riccò, B. A portable electronic system for in-situ measurements of oil concentration in MetalWorking fluids. *Sens. Actuators A Phys.* **2016**, *243*, 7–14. [CrossRef]
12. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of things: Security and solutions survey. *Sensors* **2022**, *22*, 7433. [CrossRef] [PubMed]
13. Grossi, M.; Alfonsi, F.; Prandini, M.; Gabrielli, A. A Highly Configurable Packet Sniffer Based on Field-Programmable Gate Arrays for Network Security Applications. *Electronics* **2023**, *12*, 4412. [CrossRef]
14. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics* **2022**, *11*, 3330. [CrossRef]
15. Grossi, M.; Alfonsi, F.; Prandini, M.; Gabrielli, A. A high throughput Intrusion Detection System (IDS) to enhance the security of data transmission among research centers. *J. Instrum.* **2023**, *18*, C12017. [CrossRef]
16. Ahvanooey, M.T.; Zhu, M.X.; Li, Q.; Mazurczyk, W.; Choo, K.K.R.; Gupta, B.B.; Conti, M. Modern authentication schemes in smartphones and IoT devices: An empirical survey. *IEEE Internet Things J.* **2021**, *9*, 7639–7663. [CrossRef]
17. El-Hajj, M.; Mousawi, H.; Fadlallah, A. Analysis of lightweight cryptographic algorithms on iot hardware platform. *Future Internet* **2023**, *15*, 54. [CrossRef]
18. Alhamarneh, R.A.; Mahinderjit Singh, M. Strengthening Internet of Things Security: Surveying Physical Unclonable Functions for Authentication, Communication Protocols, Challenges, and Applications. *Appl. Sci.* **2024**, *14*, 1700. [CrossRef]
19. Hemavathy, S.; Bhaaskaran, V.K. Arbiter PUF—A review of design, composition, and security aspects. *IEEE Access* **2023**, *11*, 33979–34004. [CrossRef]
20. Sánchez-Solano, S.; Rojas-Muñoz, L.F.; Martínez-Rodríguez, M.C.; Brox, P. Hardware-Efficient Configurable Ring-Oscillator-Based Physical Unclonable Function/True Random Number Generator Module for Secure Key Management. *Sensors* **2024**, *24*, 5674. [CrossRef]
21. Cao, R.; Mei, N.; Lian, Q. Method for improving the reliability of SRAM-based PUF using convolution operation. *Electronics* **2022**, *11*, 3493. [CrossRef]
22. Zhang, J.L.; Qu, G.; Lv, Y.Q.; Zhou, Q. A survey on silicon PUFs and recent advances in ring oscillator PUFs. *J. Comput. Sci. Technol.* **2014**, *29*, 664–678. [CrossRef]
23. Azhar, M.J.; Amsaad, F.; Köse, S. Duty-cycle-based controlled physical unclonable function. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2018**, *26*, 1647–1658. [CrossRef]
24. LTSpice Circuital Simulator. Available online: https://www.analog.com/en/resources/design-tools-and-calculators/ltspice-simulator.html (accessed on 25 June 2024).
25. Measures of Association for Contingency Tables. Available online: https://web.pdx.edu/~newsomj/cdaclass/ho_phi.pdf (accessed on 25 June 2024).

26. Liu, C.; Cao, Y.; Chang, C. ACRO-PUF: A Low, Reliable and Aging-Resilient Current Starved Inverter-Based Ring Oscillator Physical Unclonable Function. *IEEE Trans. Circuits Syst.-I* **2017**, *64*, 3138–3149. [CrossRef]
27. SN74HC00N Four 2-Input NAND Logic Gates in 180nm CMOS Technology. Available online: https://www.ti.com/product/SN74HC00 (accessed on 25 June 2024).
28. TDS 2012B Digital Oscilloscope Datasheet. Available online: https://www.sglabs.it/public/TEK_TDS2000B_series.pdf (accessed on 9 September 2024).