sensors

MDPI

Article

Ultra-Low-Power FinFETs-Based TPCA-PUF Circuit for Secure IoT Devices

Cancio Monteiro [1,*] and Yasuhiro Takahashi [2]

[1] Department of Electronics and Electrical Engineering (EEE), Faculty of Engineering, Science and Technology, Universidade Nacional Timor Lorosa'e (UNTL), Avenida Hera, Cristo-Rei, Dili 314, Timor-Leste
[2] Department of Electrical, Electronic and Computer Engineering, Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu-shi 501-1193, Japan; yasut@gifu-u.ac.jp
* Correspondence: cancio.monteiro@untl.edu.tl; Tel.: +670-73552907

Abstract: Low-power and secure crypto-devices are in crucial demand for the current emerging technology of the Internet of Things (IoT). In nanometer CMOS technology, the static and dynamic power consumptions are in a very critical challenge. Therefore, the FinFETs is an alternative technology due to its superior attributes of non-leakage power, intra-die variability, low-voltage operation, and lower retention voltage of SRAMs. In this study, our previous work on CMOS two-phase clocking adiabatic physical unclonable function (TPCA-PUF) is evaluated in a FinFET device with a 4-bits PUF circuit complexity. The TPCA-PUF-based shorted-gate (SG) and independent-gate (IG) modes of FinFETs are investigated under various ambient temperatures, process variations, and ±20% of supply voltage variations. To validate the proposed TPCA-PUF circuit, the QUALPFU-based Fin-FETs are compared in terms of cyclical energy dissipation, the security metrics of the uniqueness, the reliability, and the bit-error-rate (BER). The proposed TPCA-PUF is simulated using 45 nm process technology with a supply voltage of 1 V. The uniqueness, reliability, and the BER of the proposed TPCA-PUF are 50.13%, 99.57%, and 0.43%, respectively. In addition, it requires a start-up power of 18.32 nW and consumes energy of 2.3 fJ/bit/cycle at the reference temperature of 27 °C.

Keywords: physical unclonable function (PUF); secure keys; FinFETs; low power; adiabatic; reliable and unique identity; IoT security; SRAM PUF

check for updates

Citation: Monteiro, C.; Takahashi, Y. Ultra-Low-Power FinFETs-Based TPCA-PUF Circuit for Secure IoT Devices. *Sensors* **2021**, *21*, 8302. https://doi.org/10.3390/s21248302

Academic Editors: Akhilesh Tyagi and Himanshu Thapliyal

Received: 17 November 2021
Accepted: 9 December 2021
Published: 11 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 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 (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, the emerging Internet of Things (IoT) technology has simultaneously introduced challenges and opportunities for engineering-related fields. IoT devices include smartphones, smart cards, biomedical devices, radio frequency identification (RFID) tags, and many other cryptographic devices that require security characteristics, such as authenticity, integrity, and confidentiality in performing their tasks [1,2]. Security is one of the main current challenges for IoT [3–6] as it begins to materialize in our daily life and future industrial systems (Industry 4.0) [7]. IoT devices must face several tough challenges, such as low energy consumption, lack of computational resources [8,9], as well as the need to secure devices against cyber-attacks [10]. Authentication, authorization, and privacy are three sides of the security triangle in IoT. Authentication is the first barrier in front of cyber-attacks. Physical unclonable functions (PUFs) have been proposed as a lightweight, cost-efficient, and ubiquitous solution. Importantly for IoT developers, PUFs promise to achieve perfectly secure authentication without any cryptographic assets on the device, which makes them especially interesting for resource-scarce IoT devices [11,12]. The characteristics of a PUF include unpredictable response (R) as an output of the system owing to intrinsic variations, which are stimulated by the input challenge (C). The challenge–response system is modeled as a black box; hence, the PUF input–output relation is described as R = f(C), where f(.) is an unknown internal parameter influenced by the

intrinsic variations of the device [13,14]. Practically, no two chips generate identical responses for a particular challenge, as depicted in Figure 1. The combination of a challenge and its corresponding response is called a challenge response pair (CRP).

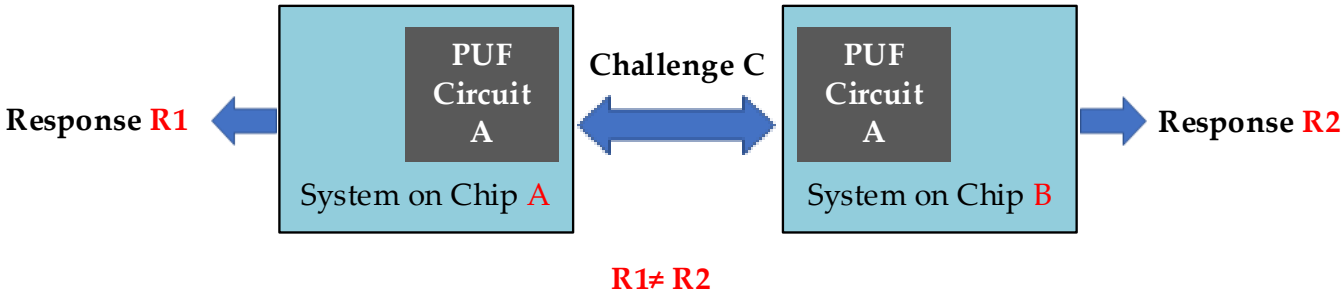


Figure 1. Two identical PUF circuits on two different chips generate different responses (modified from [15]).

The PUF security metrics (the stability, the reliability, and the uniqueness) and the low power requirement have triggered enormous studies at the PUF cell level, such as investigations on the arbiter PUF [16–18], ring-oscillator (RO) PUF [19–24], be-stable ring PUF [25], glitch PUF [26], dynamic random access memory (DRAM) PUF [27,28], and static random access memory (SRAM) PUF [29,30]. In addition, many studies on low-power PUF circuits have been conducted, such as robust digital response and low-power current-based PUF [31], as well as the SRAM-based PUFs, over a wide range of supply voltages from the super-threshold voltage regime down to the near-threshold voltage (NTV) regime [32]. It has to be noted that the IoT devices are mostly battery-powered embedded devices and operate in low-frequency ranges. Meanwhile, all PUF cells presented in [16–30] undergo high-power consumption and voltage ramp-up time adaptation for a reliable PUF circuit [33]. To address for low-power and stable PUF security profiles, the low-power technique of the adiabatic switching principle [34] has been adopted in SRAM style PUF cell design [33,35].

Continuous scaling-down of planar MOSFETs over the past four decades has delivered ever-increasing transistor density into integrated circuits (ICs). However, continuing this trend in the nanometer regime is very challenging due to the drastic increase in the subthreshold leakage current (*I*off) [36–38]. Due to the very narrow channel lengths in deeply scaled MOSFETs, the drain potential begins to influence the electrostatics of the channel and, consequently, the gate loses adequate control over the channel. As a result, the gate is unable to shut off the channel completely in the off-mode of operation, which leads to an increased *I*off between the drain and the source [39]. Very limited work on employing FinFET-based PUF has reported, such as FinFET-based hybrid ring arbiter PUF [40] and oscillator collapse and time collapse comparator PUFs [41].

In this work, a novel study on FinFET-based SRAM PUF is presented. The previous work on two-phase clocking adiabatic PUF (TPCA-PUF) [33] cells is investigated using the dual-gate FinFET 45 nm process with 1.0 V nominal supply voltage. The uniqueness, reliability, and the BER of the proposed TPCA-PUF are compared with the QUALPUF [35] using the same process technology.

The remainder of this paper is structured as follows: Section 2 introduces the FinFET-based adiabatic PUF by first explaining the fundamental adiabatic logic current trace compared to the traditional logic style, FinFET physical structures, the proposed FinFET adiabatic PUF, and its implementation into 4-bits LSI PUF. The simulation conditions, security evaluation metrics, and simulation results are described in Section 3. The evaluation of the proposed work in comparison with conventional PUFs is discussed in Section 4. Finally, Section 5 concludes the research findings of this work.

2. Adiabatic FinFET-Based PUF

2.1. Adiabatic Logic

Adiabatic switching is commonly used for minimizing the energy lost during the charging/discharging period at all nodes of the circuit. The main concept of adiabatic switching is shown in Figure 2b, which indicates a transition that is considered sufficiently slow such that heat is not significantly emitted. The adiabatic dissipated energy is expressed as:

$$E_{Adiabatic} = \frac{RC}{\tau} CV_{dd}^2 \quad (1)$$

where R is the effective resistance in the driven device, C is the output node capacitance to be switched, τ is the time over which switching occurs, and V_{dd} is the voltage to be switched across. Ideally, the charging energy, $E_{Adiabatic}$, tends to zero by increasing the length of τ. Conversely, the conventional CMOS logic operation is shown in Figure 2a, with the following equation:

$$E_{CMOS} = \frac{1}{2} CV_{dd}^2 \quad (2)$$

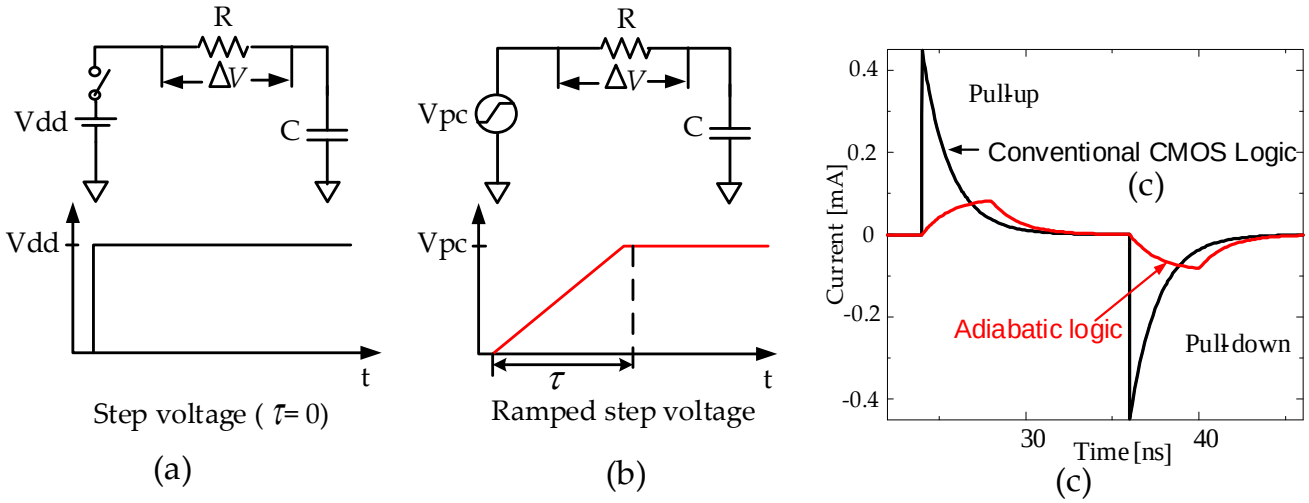


Figure 2. Comparison of the supply currents for the equivalent RC models: (**a**) CMOS logic with step voltage, (**b**) adiabatic logic with ramped step voltage, and (**c**) the peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic under the same parameters and conditions.

Here, in Equation (2), it is possible to reduce the charging energy only by reducing Vdd or capacitor, C. Figure 2c shows a comparison of the peak supply current for the equivalent RC models of the conventional CMOS logic versus the adiabatic logic. The comparison result in this figure shows that the instantaneous peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic style.

2.2. Fundamental of FinFET

With the scaling down of the transistor conductive channel, the short-channel effects (SCEs) become intolerable, and many multi-gate devices have been proposed to overcome the SCEs. Due to the relatively simple manufacturing process and the good compatibility with bulk CMOS, FinFET is considered to be a double gate (front gate and back gate) that can replace the high k of the planar MOSFET. The FinFET device has the advantages of higher on-state current, lower off-state current (lower leakage current), and faster switching speed [42]. The unique characteristic of the FinFET is that the conducting channel consists of thin silicon, known as "fin", which forms the body of the device. Moreover, FinFET is also known as a non-planner double-gate MOSFET (DG-MOSFET), in which both the front gate (FG) and back gate (BG) are tied together. A typical FinFET structure is shown in Figure 3, in which Figure 3a,b depict the three-dimensional structure and cross-sectional

top view of the FinFET, respectively. Figure 3c demonstrates the schematic symbol with shorted-gate (SG) mode and independent-gate (IG) mode of the n-type and p-type FinFETs. Furthermore, according to front gate and back gate being tied up or not, FinFET circuits can be divided into three different operating modes, namely, SG, IG, and the low-power gate (LP) modes [43].

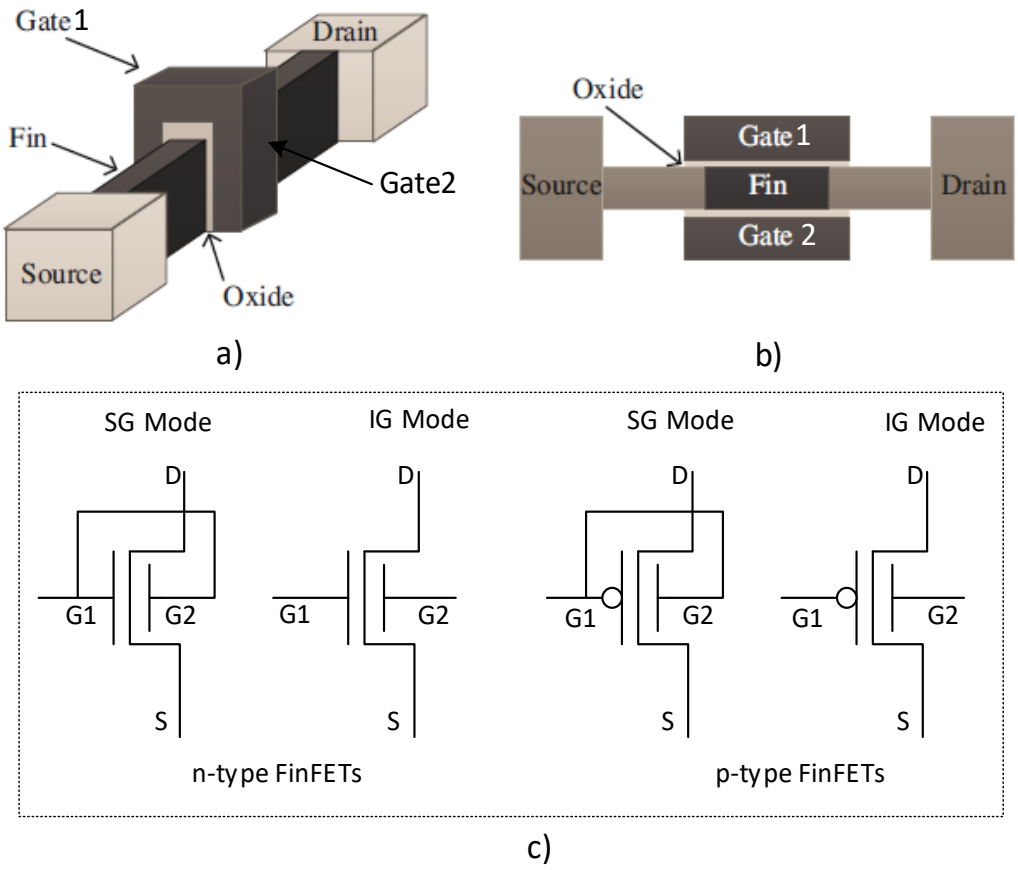


Figure 3. FinFET model and schematic: (**a**) three-dimensional structure, (**b**) cross-sectional top view, and (**c**) schematic symbol (modified from [42]).

2.3. Adiabatic FinFET TCPA-PUF

The proposed FinFET-based TPCA-PUF circuit topology is shown in Figure 4. The CMOS-based TCPA-PUF was proposed in [33], which is adiabatically operated in four phases (wait, evaluate, hold, and recover phases). It consists of a static CMOS inverter (P1 and N1), which plays a key role in charging and discharging the PUF cell semi-adiabatically using a trapezoidal power clock signal of Vpc and controlled by the Cb. Similar to the QUALPUF circuit [35], the proposed TCPA-PUF cell consists of a cross-coupled inverter (P2, P3, N2, and N3) to evaluate the response-bits (output nodes of Rb and Rb- in Figure 4). As an improvement from the QUALPUF one, the current flow from one of the output nodes is controlled to slowly flow to the ground through transistor N4, by controlling its operation speed with a ramped Vpc- signal.

In this work, the same circuit topology is then further investigated using bulk-type FinFETs in SG mode to limit the leakage current that may flow through static inverter P1 and N1 transistors. To the best of our knowledge, this is the first work on SRAM-based FinFET PUF cells in adiabatic operation for ultra-low-power and high performance (security metrics) for secure key generation and/or other related weak PUF application.

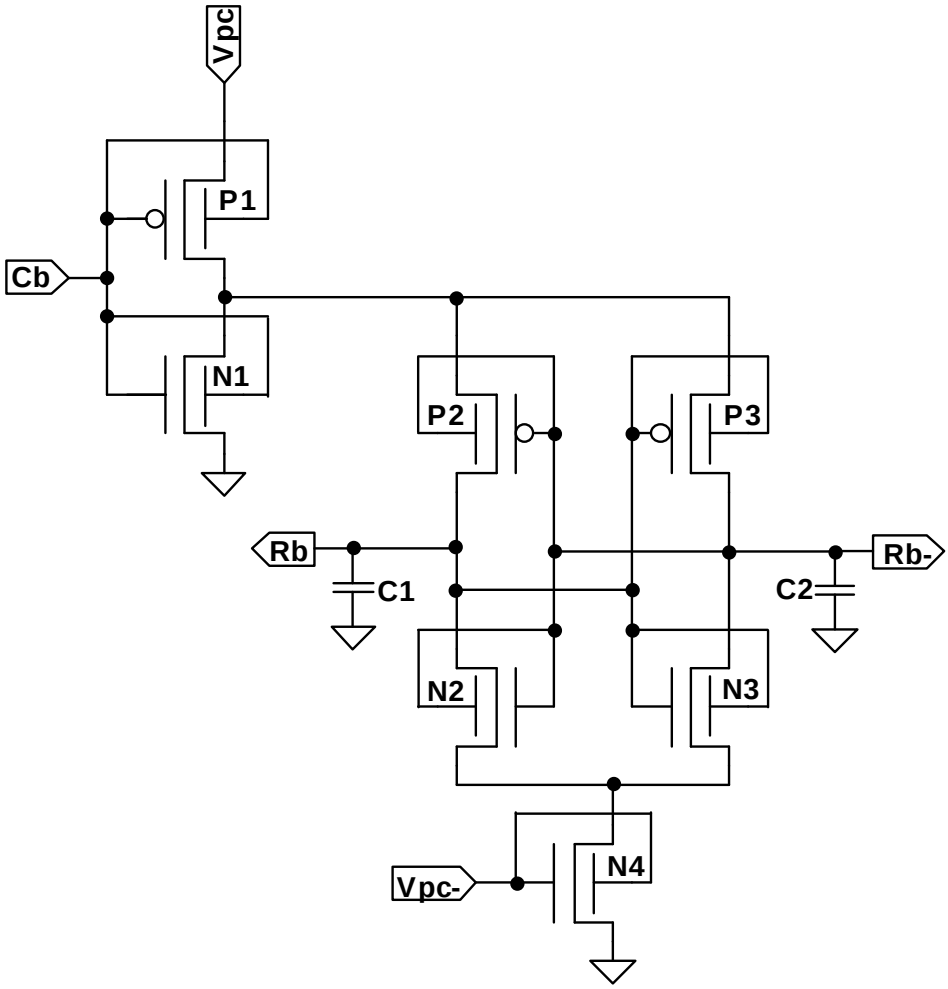


Figure 4. Proposed SRAM-based FinFET TPCA-PUF circuit.

2.4. 4-Bits Adiabatic FinFET TPCA-PUF

To validate the proposed FinFET TPCA-PUF cell, we have designed a 4-bits cascaded adiabatic PUF, as depicted in Figure 5. Each local PUF is supplied by 4 power clocks, where each adjacent clock differs by a phase difference of 90°. For instance, if the first cell, as shown in Figure 5, is operating in the hold phase, the next cell in the same local PUF is operating in the recovery phase. Similarly, the other two PUFs are operating in the wait phase and the evaluate phase, respectively. When all 4 outputs are sampled simultaneously, it leads to a 4-bit-length. Moreover, each local PUF cell is controlled by challenge bits, and each adjacent bit has a $\frac{1}{4}$ delay time of one power clock cycle. This means that if one cycle of the Vpc signal is 10 ns, then the second *Cb* signal has a 2.5 ns delay time compared to the first *Cb* signal. This delay time allows the challenge bits to flip the response signals right at the middle point of the idle/wait phase of the Vpc signals, and the challenge bits are perfectly flipped adiabatically, and as result of this, the energy is significantly reduced, as reported in [33].

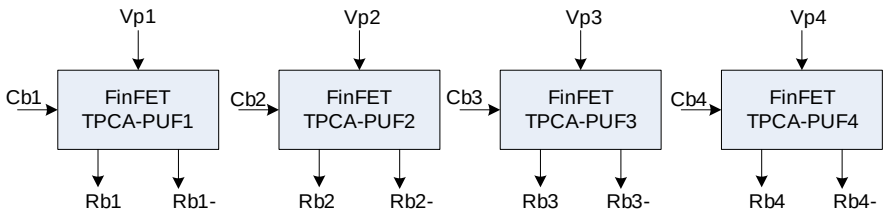


Figure 5. Proposed 4-bits FinFET TPCA-PUF architecture.

Monte-Carlo simulation result of the 4-bits TPCA-PUF and QUALPUF challenge–response signals are depicted in Figure 6. This result was obtained with a reference temperature of T = 27 °C and C_L = 10 fF, f_{Cb} = 10 MHz, and f_{Vpc} = 100 MHz, with ±10% of Vth variation. The simulation results of response signals (Rb1–Rb4) with the given challenge bit (Rb) showed correct and stable operation for both PUF circuit topologies.

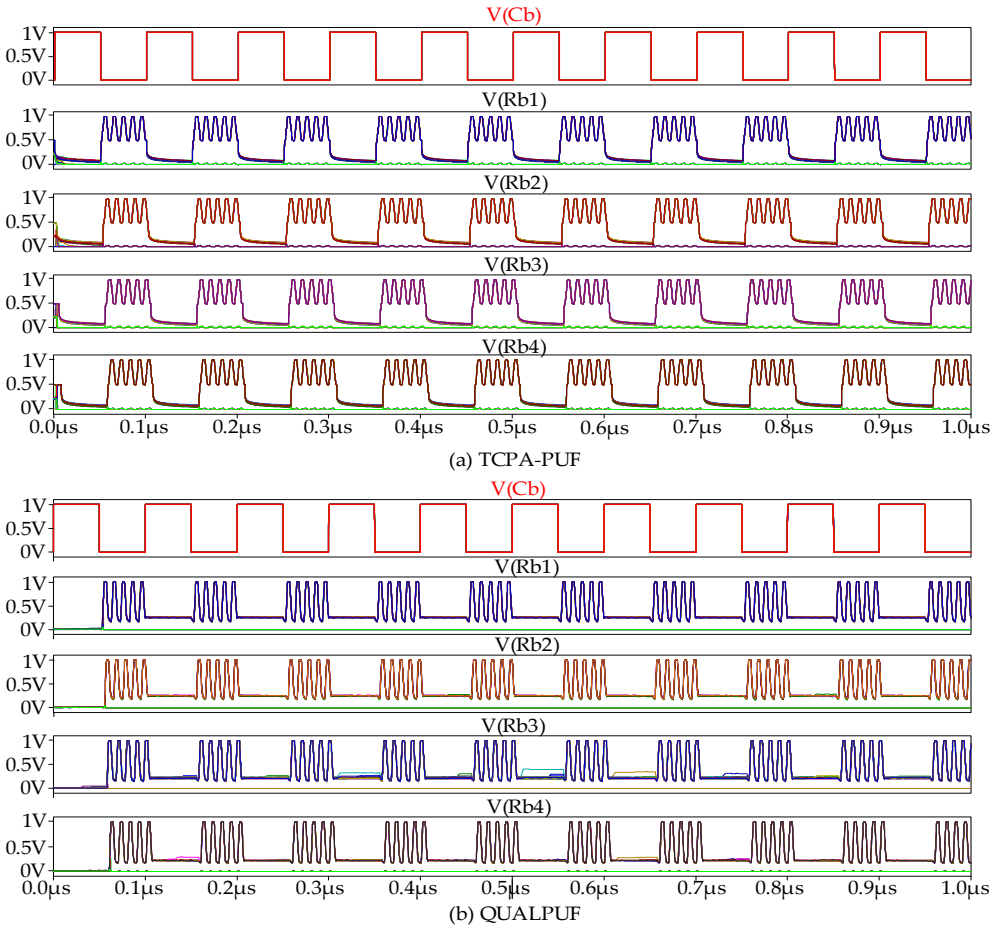


Figure 6. 4-bits LSI circuit Monte-Carlo simulation result: (**a**) proposed FinFET-based TPCA-PUF and (**b**) FinFET-based QUALPUF.

3. Simulation and Results

3.1. Simulation Condition

To analyze the effectiveness of the proposed FinFET-based TPCA-PUF, the 4-bit cascaded PUF was simulated using a 45 nm bulk FinFET standard process. Table 1 summarizes the device parameters and the simulation conditions.

Table 1. Simulation conditions.

Power supply	- Vpc: swing from 0.5 to 1.0 V trapezoidal clock, f_{Vpc} = 100 MHz - Vpc-: swing from 0 to 0.5 V trapezoidal power clock, f_{Vpc-} = 100 MHz - *Cb* voltage: 1.0 pulse signal, f_{Cb} = 10 MHz
Transistor parameter	- 45 nm double-gate FinFET process

For the ability of PUF to uniquely distinguish a chip among the group of other chips, 100 runs of the Monte-Carlo simulation were conducted to emulate the behavior of 100 IC

PUF chips. This simulation aimed to analyze the effects of the process variation, such as threshold voltage (V_{TH}) variation, the gate oxide thickness (T_{OX}) variation, and the ambient temperature variation. The ±10% tolerance variation (for V_{TH} and T_{OX}) was set for the Monte-Carlo simulation condition to evaluate the uniqueness and the reliability of the proposed adiabatic PUF cell. Moreover, the ±20% of supply voltage was applied to further investigate the reliability of the proposed TPCA-PUF circuit. The temperature variation was set at −40, 0, 27, 50, and 100 °C.

3.2. Simulation Result

The relationship of input challenge bits and the output response bits of the proposed FinFET-based TPCA-PUF cell is in correct function, as depicted in Figure 6. For performance analysis, two major evaluation results are presented in this section: the energy dissipation per cycle per challenge bits (logic "1" and "0"), and the PUF evaluation metrics of uniqueness, reliability, and the bit-error-rate (BER).

3.3. Energy dissipation

One of the major reasons for employing adiabatic switching techniques in PUF circuits is to reduce power consumption. In this study, the energy is collected from the total instantaneous power along the duration of the challenge bits cycle, as follows:

$$E = \int_0^T \Sigma(VpcsIpcs)dt \tag{3}$$

where T signals the period of the challenge bits (f_{Cb} = 10 MHz or inversely equal to 100 ns). Energy dissipation of 4-bits TCPA-PUF is depicted in Figure 7. Figure 7a,b depict an energy consumption comparison for ±10% tolerance variation of T_{OX} and V_{TH}, respectively, for a load capacitance that varies from 10 to 200 fF. The results show that the proposed FinFET-based TPCA-PUF consumes lower energy compared to the QUALPUF topology [35].

3.4. PUF Evaluation Metrics

We utilized three evaluation metrics to verify the proposed adiabatic PUF behavior.

(1) The Uniqueness: Used to determine the ability of a PUF to uniquely distinguish a chip among the other chips [35]. The ideal value of the uniqueness metric is 50%. The uniqueness is expressed as:

$$\text{Uniquness}(\%) = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i,\ R_j)}{n} \times 100 \tag{4}$$

where $HD(R_i, R_j)$ represents the Hamming Distance of two different PUF instances' responses, with k = number of chips and n = bit-length.

(2) The Reliability: Measures the reproducibility of the challenge–response pairs of a PUF instance with the varying environmental conditions, such as temperature and process variations. The reliability is mathematically expressed as:

$$\text{Reliability}(\%) = 100 - \frac{1}{k} \sum_{i=1}^{k} \frac{HD(R_i,\ R_{i,j})}{n} \tag{5}$$

where k represents the total number of chips (k = 100 in this work), n is the number of PUF bits, and $HD(R_i, R_{i,j})$ is the Hamming Distance of j-th sampling of R_i. The ideal value of the reliability is 100%.

(3) Bit-Error-Rate (BER): Indicates the error rate of the reliability of a PUF circuit. The ideal performance of the reliability is 100%. However, it is difficult to achieve in practice. BER is expressed as:

$$\text{BER}(\%) = 100 - \text{Reliability}(\%) \tag{6}$$

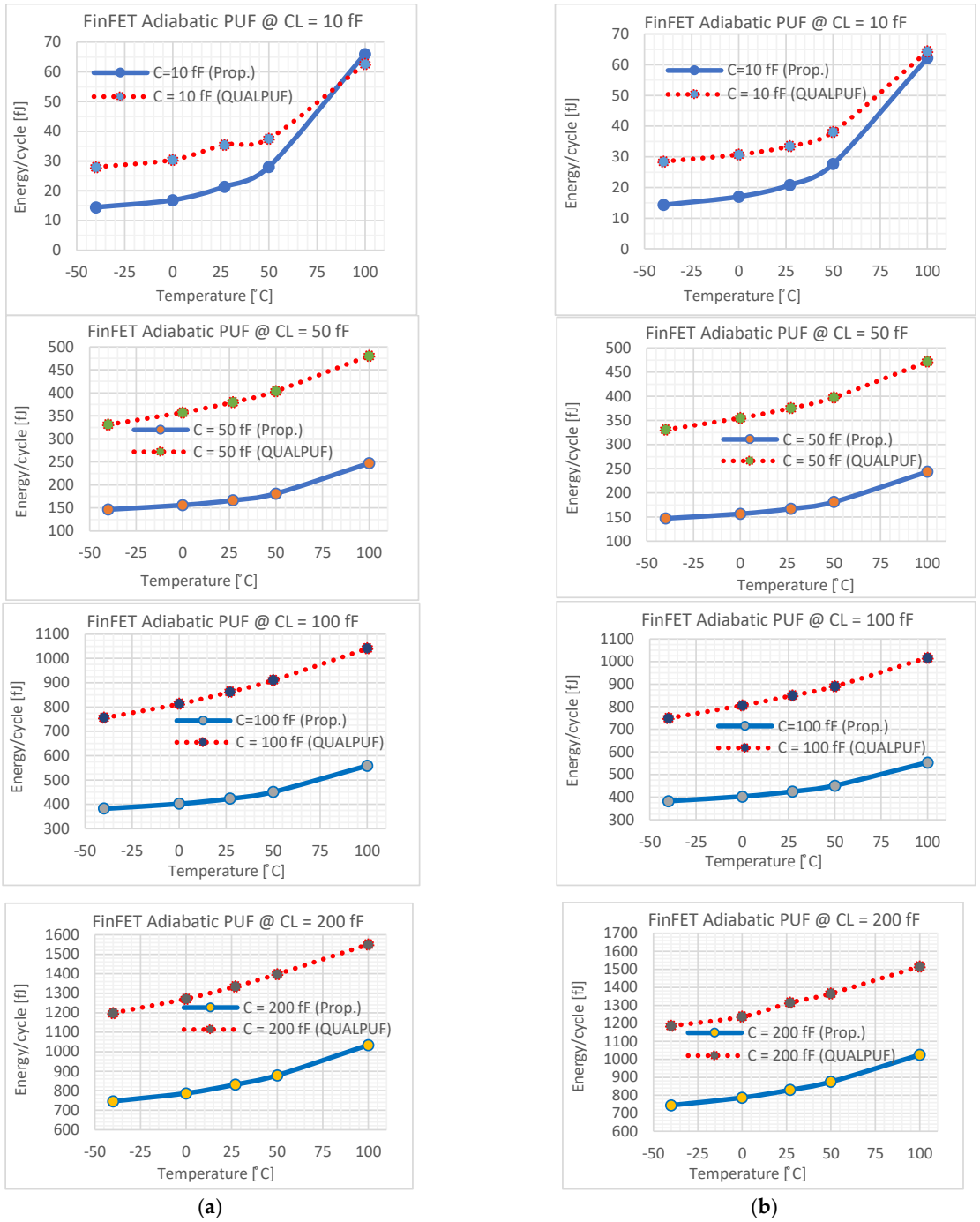


Figure 7. Energy consumption: (**a**) 10% of TOX variation and (**b**) 10% of V_{TH} variation, with load capacitance varying from 10 to 200 fF.

To enable the calculation of uniqueness, reliability, and the BER (Equations (2)–(4)), we conducted Monte-Carlo simulations with bit size of $n = 4$, and the chip number of $k = 100$. The calculation result of the uniqueness is graphically depicted in Figure 8, and the results of the reliability and the BER are shown in Figures 9 and 10, respectively, all under the condition of $\pm 10\%$ V_{TH} variations. Output nodes' capacitors also vary from 10 to 200 fF to emulate the practical chip connection. In Figures 8–10, the solid lines depict the proposed FinFET-based TPCA-PUF and the dotted lines show the FinFET-based QUALPUF.

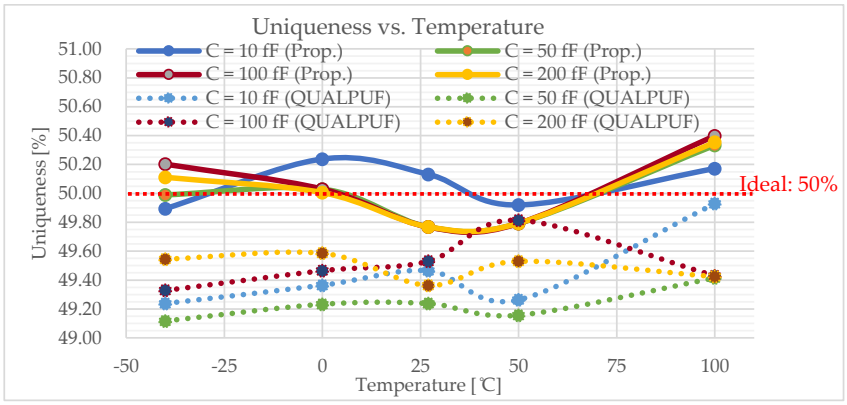


Figure 8. Uniqueness of the proposed FinFET-based TPCA-PUF (labeled as Prop.) versus QUALPUF under the V_{TH} variation (4-bit PUF).

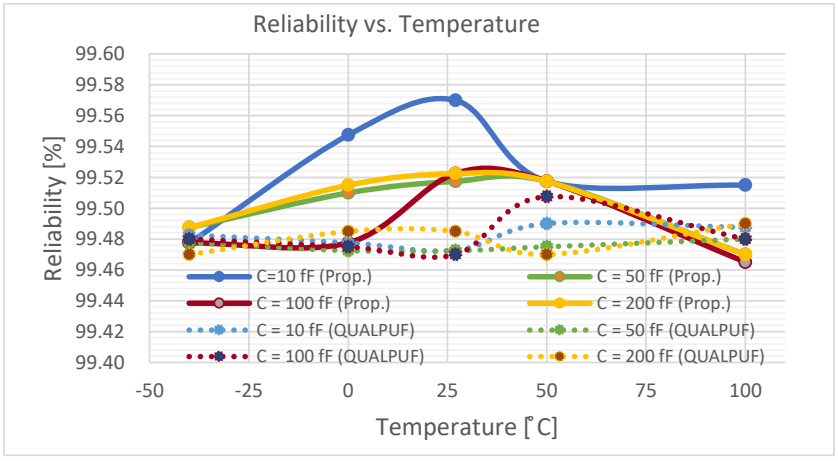


Figure 9. Reliability of the proposed FinFET-based TPCA-PUF (labeled as Prop.) versus QUALPUF under the V_{TH} variation (4-bit PUF).

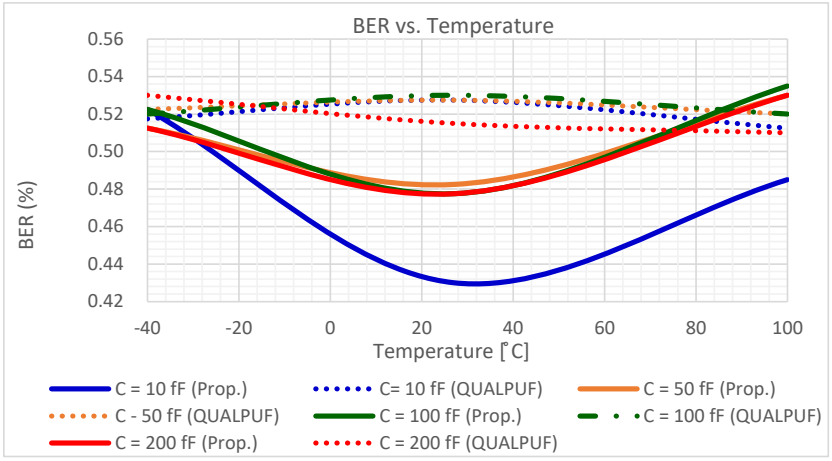


Figure 10. The BER of the proposed FinFET-based TPCA-PUF (labeled as Prop.) versus QUALPUF under the V_{TH} variation (4-bit PUF).

4. Supply Voltage Variation

Unexpected supply voltage fluctuation may also affect the reliability of any PUF performance. Hence, we have also further evaluated the reliability of the proposed adiabatic PUF against supply voltage variations. The 100 PUF instances were simulated under

different supply voltages from 0.8, 1.0, and 1.2 V, for 45 nm bulked FinFET technology, and at three different temperatures of −40, 27, and 100 °C. The responses were read with 1.0 V as a reference, and then BER was calculated, as depicted in Figure 11. This figure indicates that the proposed TPCA-PUF cells are more resilient and stable under supply voltage variation at around normal temperatures.

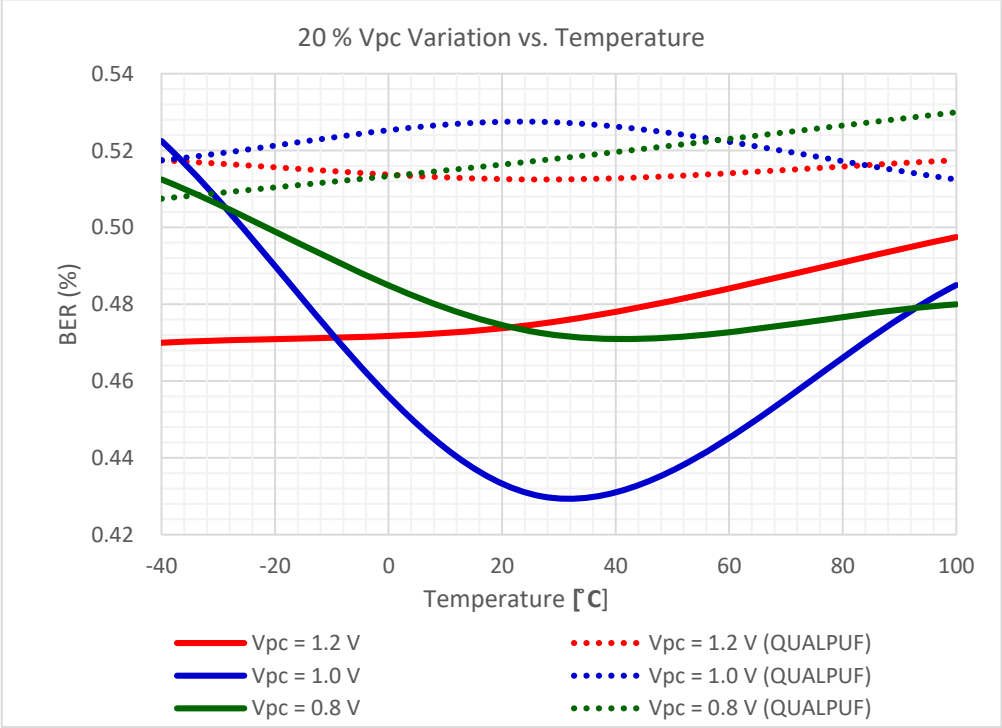


Figure 11. The BER of the proposed FinFET-based TPCA-PUF (labeled as Prop.) versus QUALPUF under the ±20% supply voltage variation (4-bit PUF).

5. Discussion

It has been revealed that the FinFET device has several advantages, such as higher on-state current, lower off-state current (lower leakage current), faster switching speed, and its double dual gates, enabling three possible connection modes (SG, IG, and LP) for low-power and high-speed applications. In this work, we have investigated the proposed TPCA-PUF cell using bulk FinFET with the 45 nm process for all SG, IG, and LP modes. As a result, we have found that SG mode is suitable for the proposed TPCA-PUF circuit topology. The gate connection type of LP and IG modes led to higher energy and produced the wrong response bits for a larger cascaded bit-length (4-bits in this work). Therefore, the whole work in this paper has utilized the SG mode connection type (refer to Figure 4).

The TPCA-PUF cell was implemented using SRAM-based circuit topology, and hence this study is claimed to be the first work in the literature employing FinFET-based SRAM-type PUF. Consequently, the previous reports of SRAM-based QUALPUF and TPCA-PUF [33,35] were re-simulated in the FinFET 45 nm process, as depicted in Figures 7–11, and the key performances are described in Table 2. From Figures 7–11, we can observe that the proposed FinFET-based TPCA-PUF demonstrated its superior performance (for both power and security metrics). Numerical data in Table 2 compare the QUALPUF and proposed TPCA-PUF, and more specifically, columns 4 and 6 demonstrate the simulation and calculation results from the current work (using the same parameters of the FinFET 45 nm process). Overall, data have shown that although FinFET-based QUALPUF and TPCA-PUF perform similar security metrics, the proposed TPCA-PUF consumes lower energy/bit/cycle and start-up power, which is suitable for low-power IoT applications.

Table 2. Comparison of conventional and proposed adiabatic PUFs (with T = 27 °C and C_L = 10 fF, f_{Cb} = 10 MHz, and f_{Vpc} = 100 MHz).

PUF	QUALPUF [35]			TCPA-PUF	
	CMOS		FinFET	CMOS	FinFET
Year	2020		This Work	2021 [33]	This Work
Tech. Process (nm)	180 nm	45 nm	45 nm	180 nm	45 nm
Topology	Adiabatic SRAM			Adiabatic SRAM	
Transistor number/bit	5	5	5	7	7
Start-up power	3.08 µW	NA	65.69 nW	0.47 µW	18.32 nW
Energy (fJ/bit/cycle)	39.18	0.08	7.36	15.98	2.30
Uniqueness (%)	40.50	49.41	49.46	49.82	50.13
Reliability (%)	96.20	99.60	99.47	99.47	99.57
BER (%)	3.8	0.4	0.53	0.53	0.43

6. Conclusions

In this study, we have presented an investigation study on SRAM-based FinFET PUF using the 45 nm technology process. The previous proposed TPCA-PUF was further investigated in a 4-bits cascaded bit-length, where the evaluation metrics of power consumption, the uniqueness, reliability, and the BER have been reported. For the low-power requirement, the proposed TPCA-PUF has reduced energy/bit/cycle and start-up power, both by about 70% compared to the QUALPUF cell at the same reference temperature of 27 °C.

The uniqueness, reliability, and the BER of the proposed FinFET-based TPCA-PUF were 50.13%, 99.57%, and 0.54%, which shows a superior security performance if compared with the FinFET-based QUALPUF cell. The remarkable performance (ultra-low power and security profile) of the proposed FinFET-based TPCA-PUF makes it an appropriate candidate for low-power and secure IoT device applications.

Further studies will be addressed to investigate the proposed TPCA-PUF with 128-bits, and address LSI implementations.

Author Contributions: C.M. and Y.T. contributed to the design of the proposed circuit; C.M. performed the simulations, and the writing—original draft. All authors participated in data analysis and paper revision. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request from the authors.

Acknowledgments: The authors would like to acknowledge the JICA-CADEFEST project for the financial support.

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

References

1. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
2. Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. *Wirel. Pers. Commun.* **2011**, *58*, 49–69. [CrossRef]
3. Keoh, S.L.; Kumar, S.S.; Tschofenig, H. Securing the internet of things: A standardization perspective. *IEEE Internet Things J.* **2014**, *1*, 265–275. [CrossRef]
4. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in internet of things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]

5. Radomirovic, S. Towards a model for security and privacy in the internet of things. In Proceedings of the First International Workshop on Security of the Internet of Things, Tokyo, Japan, 29 November–1 December 2010.
6. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.-H.; Jin, Y. Security analysis on consumer and industrial iot devices. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 519–524. [CrossRef]
7. Shrouf, F.; Ordieres, J.; Miragliotta, G. Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm. In Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Selangor, Malaysia, 9–12 December 2014; pp. 697–701. [CrossRef]
8. Martinez, B.; Montón, M.; Vilajosana, I.; Prades, J.D. The power of models: Modeling power consumption for iot devices. *IEEE Sens. J.* **2015**, *15*, 5777–5789. [CrossRef]
9. Mukhopadhyay, S.C.; Suryadevara, N.K. Internet of things: Challenges and opportunities. In *Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–17. [CrossRef]
10. Babaei, A.; Schiele, G. Spatial reconfigurable physical unclonable functions for the internet of things. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Guangzhou, China, 12–15 December 2017; pp. 312–321. [CrossRef]
11. Mukhopadhyay, D. PUFs as promising tools for security in internet of things. *IEEE Des. Test* **2016**, *33*, 103–115. [CrossRef]
12. Halak, B.; Zwolinski, M.; Mispan, M.S. Overview of PUF-based hardware security solutions for the internet of things. In Proceedings of the 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), Abu Dhabi, United Arab Emirates, 16–19 October 2016; pp. 1–4. [CrossRef]
13. Helder, C.; Yu, M.-D.; Koushanfar, F.; Devadas, S. Physical Unclonable Functions and Applications: A Tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [CrossRef]
14. Hori, Y.; Yoshida, T.; Katashita, T.; Satoh, A. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs. In Proceedings of the 2010 International Conference on IEEE Reconfigurable Computing and FPGAs, Cancun, Mexico, 13–15 December 2010; pp. 298–303. [CrossRef]
15. Babaei, A.; Schiele, G. Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. *Sensors* **2019**, *19*, 3208. [CrossRef] [PubMed]
16. Lee, J.W.; Lim, D.; Gassend, B.; Suh, G.E.; Dijk, M.v.; Devadas, S. A technique to build a secret key in integrated circuits for identification and authentication applications. In Proceedings of the 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), Honolulu, HI, USA, 17–19 June 2004; pp. 176–179. [CrossRef]
17. Beckmann, N.; Potkonjak, M. Hardware-based public-key cryptography with public physically unclonable functions. In *International Workshop on Information Hiding*; Springer: Darmstadt, Germany, 2009; pp. 206–220. [CrossRef]
18. Machida, T.; Yamamoto, D.; Iwamoto, M.; Sakiyama, K. Implementation of double arbiter PUF and its performance evaluation on FPGA. In Proceedings of the 20th Asia and South Pacific Design Automation Conference, Chiba, Japan, 19–22 January 2015; pp. 6–7. [CrossRef]
19. Maiti, A.; Casarona, J.; McHale, L.; Schaumont, P. A large scale characterization of RO-PUF. In Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, USA, 13–14 June 2010; pp. 94–99. [CrossRef]
20. Gao, M.; Lai, K.; Qu, G. A highly flexible ring oscillator PUF. In Proceedings of the 51st Annual Design Automation Conference, San Francisco, CA, USA, 1–5 June 2014; ACM: New York, NY, USA, 2014; pp. 1–6. [CrossRef]
21. 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. [CrossRef]
22. Gassend, B.; Clarke, D.; Dijk, M.v.; Devadas, S. Silicon physical random functions. In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 18–22 November 2002; pp. 148–160. [CrossRef]
23. Cao, Y.; Zhang, L.; Chang, C.-H.; Chen, S. A Low-Power Hybrid RO PUF with Improved Thermal Stability for Lightweight Applications. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2015**, *34*, 1143–1147. [CrossRef]
24. Günlü, O.; Kernetzky, T.; İşcan, O.; Sidorenko, V.; Kramer, G.; Schaefer, R.F. Secure and Reliable Key Agreement with Physical Unclonable Functions. *Entropy* **2018**, *20*, 340. [CrossRef] [PubMed]
25. Chen, Q.; Csaba, G.; Lugli, P.; Schlichtmann, U.; Ruhmair, U. The bistable ring PUF: A new architecture for strong physical unclonable functions. In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), San Diego, CA, USA, 5–6 June 2011; pp. 134–141. [CrossRef]
26. Anderson, J.H. A PUF design for secure FPGA-based embedded systems. In Proceedings of the 15th Asia and South Pacific Design Automation Conference (ASP-DAC), Taipe, Taiwan, 18–21 January 2010; pp. 1–6. [CrossRef]
27. Tehranipoor, F.; Karimian, N.; Xion, K.; Chandy, J.A. DRAM-based Intrinsic physical unclonable functions for system level security. In Proceedings of the 25th Edition on Great Lakes Symposium on VLSI, Pittsburgh, PA, USA, 20–22 May 2015; pp. 15–20. [CrossRef]
28. Tehranipoor, F.; Karimian, N.; Yan, W.; Chandy, J.A. DRAM-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2017**, *25*, 1085–1097. [CrossRef]

29. Guajardo, J.; Kumar, S.S.; Schrijen, G.-J.; Tuyls, P. FPGA intrinsic PUFs and their use for IP protection. In Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, Vienna, Austria, 10–13 September 2007; pp. 63–80. [CrossRef]
30. Holcomb, D.E.; Burleson, W.P.; Fu, K. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Trans. Comput.* **2009**, *58*, 1198–1210. [CrossRef]
31. Majzoobi, M.; Ghiaasi, G.; Koushanfar, F.; Nassif, S.R. Ultra-low power current-based PUF. In Proceedings of the 2011 IEEE International Symposium of Circuits and Systems (ISCAS), Rio de Janeiro, Brazil, 15–18 May 2011; pp. 2071–2074. [CrossRef]
32. Golanbari, M.S.; Kiamehr, S.; Bishnoi, R.; Tahoori, M.B. Reliable memory PUF design for low-power applications. In Proceedings of the 19th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 13–14 March 2018; pp. 207–213. [CrossRef]
33. Monteiro, C.; Takahashi, Y. Low-Power Two-Phase Clocking Adiabatic PUF Circuit. *Electronics* **2021**, *10*, 1258. [CrossRef]
34. Athas, W.C.; Svensson, L.J.; Koller, J.G.; Tzartzanis, N.; Chou, E.Y.-C. Low-power digital systems based on adiabatic-switching principles. *IEEE Trans. Very Large-Scale Integr. (VLSI) Syst.* **1994**, *2*, 398–407. [CrossRef]
35. Kumar, S.D.; Thapliyal, H. Design of Adiabatic Logic-Based Energy-Efficient and Reliable PUF for IoT Devices. *J. Emerg. Technol. Comput. Syst.* **2020**, *16*, 34. [CrossRef]
36. Kuhn, K.J. CMOS scaling for the 22nm node and beyond: Device physics and technology. In Proceedings of the International Symposium on VLSI Technology, Systems and Applications (VLSI-TSA '11), 25–27 April 2011; pp. 1–2. [CrossRef]
37. Roy, K.; Mukhopadhyay, S.; Mahmoodi-Meimand, H. Leakage current mechanisms and leakage reduction techniques in deep-submicrometer CMOS circuits. *Proc. IEEE* **2003**, *2*, 305–327. [CrossRef]
38. Frank, D.J.; Dennard, R.H.; Nowak, E.; Solomon, P.M.; Taur, Y.; Wong, H.-S.P. Device scaling limits of Si MOSFETs and their application dependencies. *Proc. IEEE* **2001**, *3*, 259–288. [CrossRef]
39. Bhattacharya, D.; Jha, N.K. FinFETs: From Devices to Architectures. *Adv. Electron.* **2014**, *2014*, 365689. [CrossRef]
40. Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E. Making use of semiconductor manufacturing process variations: FinFET-based physical unclonable functions for efficient security integration in the IoT. *Analog. Integr. Circ. Sig. Process.* **2017**, *93*, 429–441. [CrossRef]
41. Zayed, A.A.; Issa, H.H.; Shehata, K.A.; Ragai, H.F. Ultra-Low Power Oscillator Collapse Physical Unclonable Function Based on FinFET. *IEEE Access* **2021**, *9*, 27696–27707. [CrossRef]
42. King, T.J. FinFETs for nanoscale CMOS digital integrated circuits. In Proceedings of the IEEE/ACM International Conference on Computer-Aided Design, San Jose, CA, USA, 6–10 November 2005; pp. 207–210. [CrossRef]
43. Muttreja, A.; Agarwal, N.; Jha, N.K. CMOS logic design with independent-gate FinFETs. In Proceedings of the 25th International Conference on Computer Design, Lake Tahoe, CA, USA, 7–10 October 2007; pp. 560–567. [CrossRef]