International Journal of Nanoelectronics and Materials
Volume 14, No. 4, October 2021 [345-356]

Performance Evaluation of SRAM-PUF based on 7-nm, 10-nm and 14-nm FinFET Technology Nodes

Mohd Syafiq Mispan[1*], Aiman Zakwan Jidin[2], Hafez Sarkawi[3], and Haslinah Mohd Nasir[4]

[1,2]Micro & Nano Electronics (MiNE)
[3,4]Advance Sensors & Embedded Controls System (ASECs)
[1,2,3,4]Centre for Telecommunication Research & Innovation (CeTRI)
[1,2,3,4]Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka

Received 1 March 2021, Revised 28 June 2021, Accepted 13 July 2021

ABSTRACT

As complementary metal-oxide semiconductor (CMOS) technology continues to scale down to ultra-deep submicron (UDSM) technology, the planar metal-oxide semiconductor field-effect transistor (MOSFET) structure reaches its limit. As the channel length shrinks, the gate no longer has full control over the channel which is not desirable. The subthreshold leakage from drain to source increases as the impact over the lost control of the MOS gate terminal, and further increase the total power consumption. To ensure the continuation of CMOS scaling and to overcome the aforementioned issues, the new MOS structure which is known as fin field-effect transistor (FinFET) is introduced. On the other hand, Physical Unclonable Function (PUF) is a promising hardware-fingerprinting technology that can exploit the intrinsic process variations of CMOS technology and manifest them into unique and random binary responses. These responses can be used as a cryptographic key or device specific identifier. Nevertheless, FinFET introduces an unknown impact of its process variations towards the performance of a particular PUF. In this paper, the suitability of the FinFET technology node for a PUF as a device-specific identifier or secret key is evaluated. One of the memory-PUFs, known as static random-access memory PUF (SRAM-PUF) has been used as a case study. Three different FinFET technology nodes which are 14-nm, 10-nm, and 7-nm have been evaluated. Our findings show that the uniqueness and uniformity of SRAM-PUF still hold, closely distributed at around an ideal value of 50%. The average reliability under temperature variations of -40°C to 85°C is approximately about 98%. The reliability of SRAM-PUF responses under the V_{dd} ramp-up time variations has no significant impact although showing declining patterns at fast ramp-up time. It can be concluded that FinFET technology shows no surprises on SRAM-PUF performances.

Keywords: Physical Unclonable Function, FinFET, Process Variations, Hardware Security

1. INTRODUCTION

Physical Unclonable Function (PUF) has made its debut almost two decades ago and the research in PUF continues to progress due to its promising as hardware fingerprinting solutions for a trusted computing system. PUF exploits the intrinsic process variations during integrated circuit (IC) fabrication. The intrinsic process variations embodied in the silicon chip acts as a random function for a PUF which can uniquely map a set of challenges (given as *C*) to a set of responses (given as *R*), known as challenge response pairs (CRPs). These CRPs are random and show a device-specific property which can be applied in cryptographic key generation and IC identification and authentication applications [1].

*Corresponding author: syafiq.mispan@utem.edu.my

Several PUFs have been proposed in the literature [2, 3]. Static random-access memory PUF (SRAM-PUF) is one of the memory-based PUFs which categorized as a Weak-PUF due to limitations in its CRPs [4, 5]. SRAM-PUF has attracts a lot of attention since it has an advantage of low overhead cost in which the existing available on-chip SRAM in any computing systems can be reused as a PUF [6]. Furthermore, the simple architecture of the SRAM cell which consists of cross-coupled inverter and its vulnerability to the process mismatches has increased the wide adoption of SRAM as PUF.

The notion of PUFs is first emerged on silicon chip using Taiwan Semiconductor Manufacturing Company (TSMC) 180-nm complementary metal-oxide semiconductor (CMOS) technology node [7]. Since then, PUFs have made tremendous progress and their development has been focusing on using the conventional type of planar metal-oxide semiconductor field-effect transistor (MOSFET). Fin field-effect transistor (FinFET) technology has been introduced to overcome issues related to the short-channel effect in ultra-deep submicron (UDSM) technology such as drain-induced barrier lowering (DIBL), threshold voltage (V_{th}) roll-off, and sub-threshold leakage current. Nevertheless, the impact of its process variations on PUF functionality remains clueless as lacking study on these subject matters [8-10].

Motivated by the impact of FinFET process variations towards the performance of PUF, the focus of this paper is to analyse and evaluate the suitability of FinFET technology in PUF construction. To achieve that, we have analysed three FinFET technology nodes which are 7-nm, 10-nm, and 14-nm using a predictive technology model (PTM). We used SRAM-PUF as a case study to evaluate the performance of PUF using FinFET technology. The main contributions of this work are highlighted below:

1. We study the FinFET 6-transistor (6T) SRAM cell behaviour as PUF using 7-nm, 10-nm, and 14-nm technology nodes. We show that FinFET technologies have a significant amount of randomness in its process variations which manifested in good uniqueness and uniformity on SRAM-PUFs, close to an ideal value of 50%.
2. We study the reliability of SRAM-PUF under temperature variations of -40°C to 85°C. We found that the reliability of SRAM-PUFs using 7-nm, 10-nm, and 14-nm FinFET technology nodes is worst at -40°C with the reliability value in the range of 94% to 95%. On the other hand, the impact of V_{dd} ramp-up time variations on the reliability of SRAM-PUF has no significant impact although showing declining patterns at fast ramp-up time.

The rest of the paper is organized as follows. Section 2 describes the background which related to this work. Section 3 describes the methods used in this study. The experimental analysis and results are presented in Section 4. Finally, conclusions are drawn in Section 5.

2. BACKGROUND

2.1 SRAM-PUF

Guajardo *et al*., [4] and Holcomb *et al*., [5] proposed SRAM-PUF about the same timeline whereby they found out that existing SRAM architecture can be used as a PUF. Figure 1 illustrates the typical 6-transistor SRAM cell which comprises of a cross-coupled inverter defined as MP1, MP2, MN1, and MN2, and two access transistors defined as MN3 and MN4. The SRAM cells generate unique and random start-up values (SUVs) after the power-up process that can be used as PUF responses [11]. The transistors in SRAM cell experience V_{th} mismatches due to process variations, assuming that V_{th} of MP1 is higher compared to MP2. As the power supply rising to V_{dd} value, the current flows through the cross-coupled inverter and pulls up nodes Q and QB to V_{dd}. The charging rate of QB is higher than Q as the $V_{th,MP2} < V_{th,MP1}$. Hence, as both nodes racing towards V_{dd}, the MN1 gets turn ON and pulls down the Q node. Eventually, as the power supply reaches V_{dd}, QB settles at V_{dd}, and Q settles at 0 as depicted in Figure 2. The SUV differs from one to the other SRAM cells

(i.e., within an SRAM) and across multiple SRAM blocks due to the random nature of process variations. Hence, the SUV shows a device-specific feature which is an important characteristic to be qualified as a good PUF.

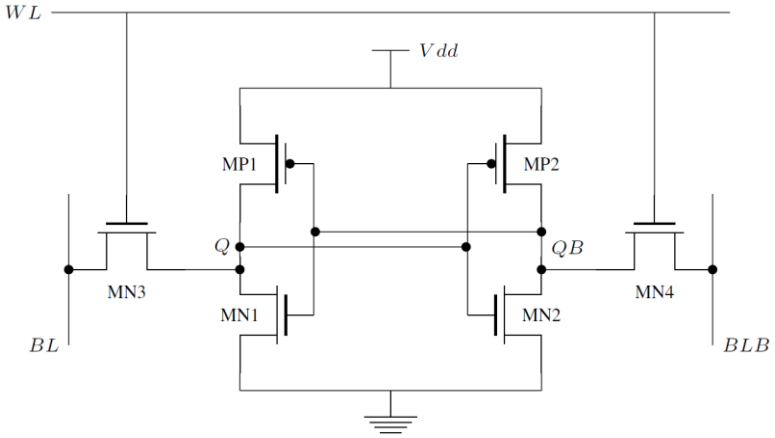


Figure 1. 6-T SRAM cell circuit

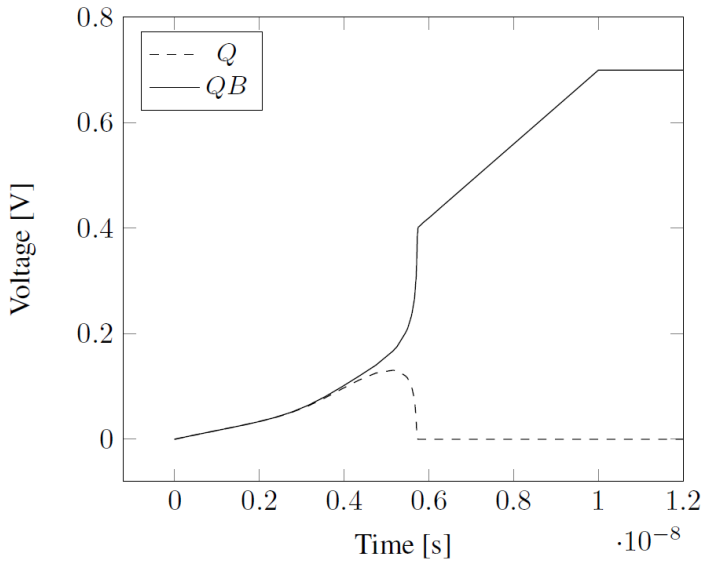


Figure 2. SRAM cell internal nodes, QB and Q settling to `1' and `0'

2.2 Related Work

Recent studies have been focusing on FinFET technology to construct new PUF architectures. Zayed *et al.*, [12] proposed a frequency divider ring oscillator PUF (FDRO-PUF) which was implemented using North Carolina State University (NCSU) process design kit (PDK) and 20-nm FinFET Predictive Technology Model (PTM) provided by Arizona State University (ASU). FDRO-PUF aims for a low power PUF design as compared to the conventional RO-PUF, taking advantage of low V_{dd} in FinFET technology. Elsewhere, Zhang *et al.*, [13] evaluated flip-flop (FF) PUFs and the test chip was fabricated at a commercial foundry using a 14/16-nm FinFET technology node. The evaluation was carried out for different types of FF such as conventional D-flip flop (DFF), Guard-Gate-based FF (GGFF), and Schmidt-Trigger-based FF (STFF). The study shows that GGFF-based PUF has the best performance as compared to the other investigated FF-based PUFs. A few more architectures based on FinFET has been proposed such as a novel speed/power optimized hybrid oscillator arbiter PUF [14], a novel memory PUF concept of 2-bit-per-cell (2B/C) using 14-

nm high-*k* metal gate (HKMG) FinFET [15], and a resistive random-access memory (RRAM) using 16-nm FinFET [16]. In another study, Yanambaka *et al*., [17, 18] proposed speed optimized hybrid oscillator arbiter PUF based on doping-less transistor FET (DLFET) and the results were compared with FinFET technology, both were using 14-nm technology node.

A few studies were focusing on SRAM-PUF based on FinFET technology. O'Uchi *et al*., [8] developed an SRAM-PUF using a polycrystalline-Si channel (poly-Si) FinFET. The comparison has been made against crystalline-Si FinFET and the result shows that poly-Si FinFET offers a better uniqueness and reliability performance on SRAM-PUF. In another study, a comparison of SRAM-PUF quality and reliability between 28-nm planar MOSFET HKMG and 16-nm FinFET has been evaluated [9]. The results show that 16-nm FinFET has promising randomness which offers better quality for SRAM-PUF. Nonetheless, the impact of aging is marginally higher in 16-nm FinFET as compared to 28-nm planar MOSFET. Elsewhere, Faragalla *et al*., [10] studied the impact of process variations on SRAM-PUF by having a linear function systematic V_{th} and Gaussian distribution random V_{th} intra-die mismatches from 5% to 15% deviations. In our study, we will focus on the impact of process variations on different technologies of FinFET which are 7-nm, 10-nm, and 14-nm technology nodes.

3. METHODOLOGY

An SRAM-PUF has been implemented using NCSU PDK and ASU PTM for 14-nm, 10-nm, and 7-nm FinFET technology nodes. Only 2048-bit of SRAM were constructed, simulated, and evaluated in this study, as it is prohibitive (i.e., time-consuming) to run a complete SRAM memory architecture. A Monte Carlo simulation is used to simulate the intrinsic variations of FinFET devices. Figure 3 illustrates the structure of a FinFET device. According to [19], the line edge roughness (LER) has a significant impact on the FinFET gate length variations. LER fluctuates the length (*L*) and the width (*tfin*) of the FinFET devices. Therefore, in our study, we set the standard deviation of *L* and *tfin* to be 3σ = 10% of the nominal value of each parameter as described in [19]. The process variations of 100 SRAM instances were modeled using a Monte Carlo simulation. The simulation was performed at a temperature 25°C and a nominal supply voltage, unless otherwise stated. The nominal values for the FinFET technology used in this study are listed in Table 1. To generate the random SUVs of SRAM cells, the supply voltage has to be ramped-up at a certain time. In this study, 1*ms* of ramp-up time of the supply voltage has been set throughout the simulation, unless otherwise stated. It is important to note that the sources of noise such as thermal noise, flicker noise, etc. have not been considered in this study.

Table 1. Nominal parameters for the nFET and pFET devices

Parameter	FinFET technology nodes		
	14-nm	10-nm	7-nm
Gate Length, *L* (nm)	18	14	11
Fin Thickness, *tfin* (nm)	10	9	7
Fin Height, *hfin* (nm)	23	21	18
Supply Voltage, V_{dd}	0.8	0.75	0.7

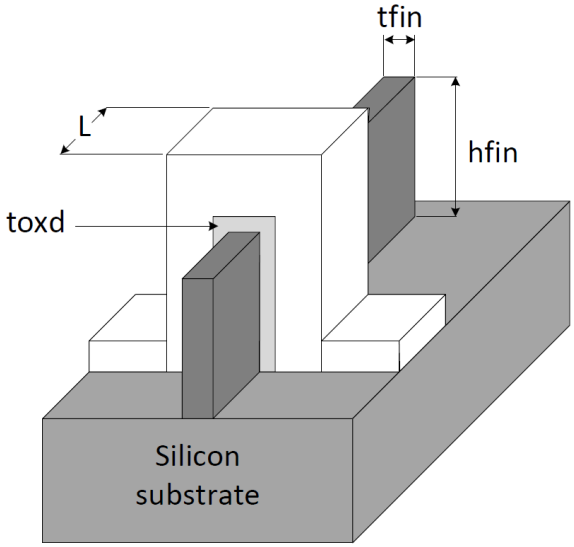


Figure 3. Illustration of a FinFET device

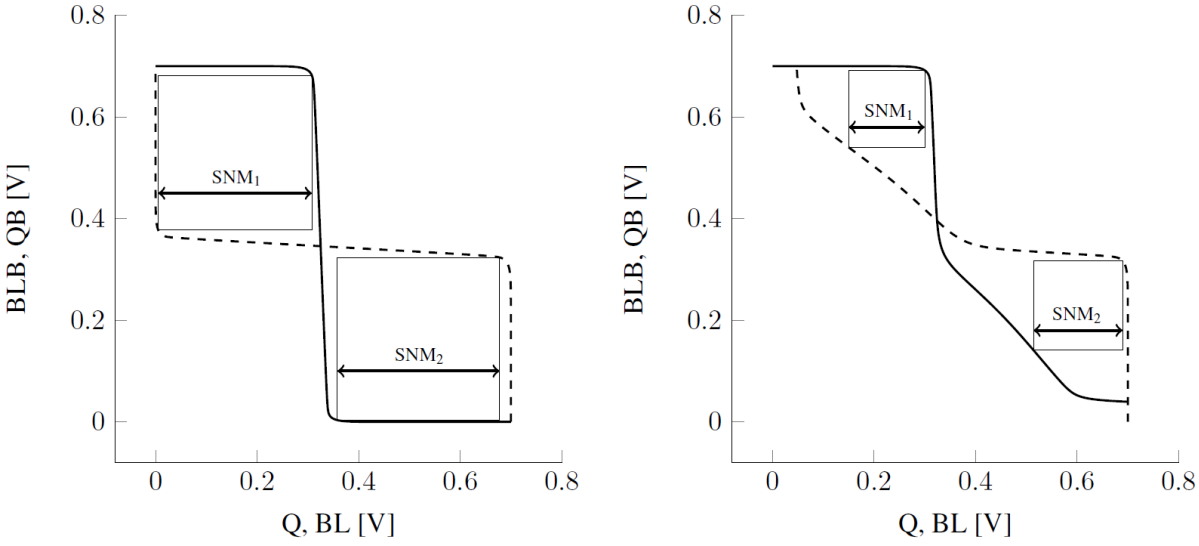
4. SIMULATION RESULTS AND ANALYSIS

The relevant simulation and analysis are discussed in this section based on the described methodology in Section 3. Further, the performance of SRAM-PUF such as uniqueness, reliability, and uniformity are quantified according to [20].

4.1 Static Noise Margin of SRAM-PUF

Static noise margin (SNM) is a metric to quantify the SRAM cell stability to retain the stored value in a bit cell during reading mode when the access transistors are ON (i.e., read SNM or RSNM) or in a hold mode (i.e., hold SNM or HSNM) [21]. An SNM of SRAM cell is defined as the minimum DC noise voltage that an SRAM cell can tolerate without flipping its state. The voltage transfer characteristic (VTC) curves of a cross-coupled inverter or also known as butterfly curve is used to determine the SNM. To compute the SNM, the largest square enclosed between two VTCs of a cross-coupled inverter first has to be found. Subsequently, the side length of this square is measured which represents the SNM. Two SNM values were yielded from SNM characterization, namely SNM1 and SNM2; therefore SNM = min (SNM1, SNM2). The characterization of RSNM and HSNM for 7-nm FinFET technology node is illustrated in Figure 4 when the word line (WL) is '1' and '0', respectively.

Table 2 summarized the HSNM and RSNM for three different FinFET technology nodes. The characterization of SNM is to determine the optimum transistor sizing of a 6-T SRAM cell. n_{fin} is referring to the number of fins which determine the width (W) of a FinFET transistor. W is computed as n_{fin} x (2 x h_{fin} + t_{fin}). PD and PU are referring to pull-down and pull-up transistors which consist of MN1 and MN2, and MP1 and MP2, respectively. Whereby, PA is referring to the access transistors, MN3 and MN4. Based on the results in Table 2, sizing of $n_{fin,\mathrm{PD}}$ = 2, $n_{fin,PU}$ = 1, and $n_{fin,PA}$ = 1 shows the optimum HSNM and RSNM for PUF applications. During the power-up of SRAM-cells, only the PU and PD transistors are involved, and these transistors must be able to retain the SUVs. The SRAM cell size is used throughout all the analysis in this study. It is also worth noting that the SNM patterns are consistent for three different FinFET technologies.



(a) HOLD SNM (b) READ SNM

Figure 4. SNM of 6-T SRAM cell for 7-nm FinFET (a) HOLD SNM measurement, *WL*=0 and (b) READ SNM measurement, *WL*=1

Table 2. Sizing ratio for optimum read and hold SNM of a 6-T SRAM cell

n_{fin}			7-nm		10-nm		14-nm	
PD	PU	PA	HSNM (mV)	RSNM (mV)	HSNM (mV)	RSNM (mV)	HSNM (mV)	RSNM (mV)
1	1	1	0.3059	0.1280	0.3281	0.1365	0.3580	0.1550
2	1	1	0.3031	0.1509	0.3246	0.1695	0.3556	0.1930
3	1	1	0.3000	0.1647	0.3213	0.1893	0.3525	0.2157

4.2 Uniqueness

The uniqueness is an important parameter to ensure the PUF functions as expected and its uniqueness close to an ideal value. When a challenge *C* is applied onto *m* similar types of PUFs, each PUF generates *n*-bit of response. Therefore, the ability to distinguish a PUF from *m* similar types of PUF is measured using Inter-hamming distance (Inter-HD), and it is given as in Eq. (1) where *i* and *j* represent two PUF instances under evaluation.

$$\text{Inter-HD} = \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD\left(R_i(n), R_j(n)\right)}{n} \times 100\% \quad (1)$$

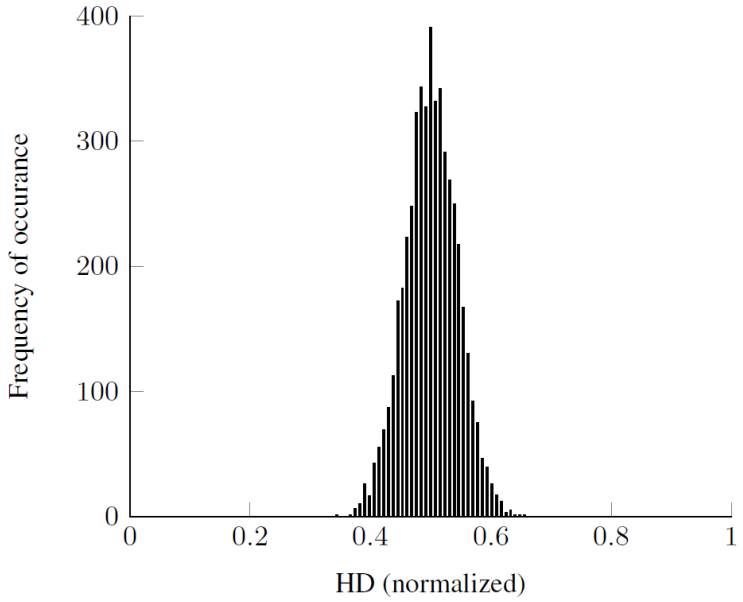


Figure 5. Uniqueness of 128-bit key for 100 SRAM-PUF instances implemented using 7-nm FinFET technology node

The uniqueness is evaluated for 128 SRAM cells for each of SRAM-PUFs, such that 128-bit is used as a cryptographic key or unique identifier. Figure 5 illustrates the uniqueness distribution, computed using Eq. (1), of the 128-bit key for 100 SRAM-PUFs which were implemented using 7-nm FinFET technology. Ideally, the uniqueness should be distributed around 50% with a very small standard deviation. The value of uniqueness and standard deviation for 7-nm, 10-nm, and 14-nm FinFET technology nodes are summarized in Table 3. As can be seen, the uniqueness is close to an ideal value of 50%, with a small standard deviation for three different FinFET technology nodes. A 50% uniqueness indicates that for a challenge applied to two or more SRAM-PUFs of a similar type, one SRAM-PUF will produce a response of about 50% unique as compared to the other SRAM-PUFs.

Table 3. Uniqueness

Technology	Uniqueness (%)	Std. Deviation
7-nm	50.08	4.36
10-nm	50.09	4.35
14-nm	50.09	4.34

4.3 Impact of Temperature Fluctuations

The ability of a PUF to reproduce the same response (i.e., applied with the same challenges) when the PUF is subjected to the environmental fluctuations such as temperature and supply voltage is measured using Intra-HD and it is given as:

$$\text{Intra-HD} = \frac{1}{m}\sum_{j=1}^{m}\frac{HD\left(R_i(n), R'_{i,j}(n)\right)}{n} \times 100\% \quad (2)$$

Based on Eq. (2), the PUF reliability can be computed, and it is defined as:

$$\text{Reliablity} = 100\% - \text{Intra-HD} \tag{3}$$

where i represents PUF under evaluation which generate n-bit response, $R_i(n)$ at nominal temperature and supply voltage, $R'_{i,j}(n)$ is the response at different condition (i.e., temperature and/or supply voltage), and m is the number of samples. According to [6, 22], the impact of the variations in the final value of the ramped-up voltage on the reliability of the SUVs is negligible. Therefore, only the temperature variations are investigated in this study. The reliability of 100 SRAM-PUFs is evaluated over the temperature range from -40°C to 85°C for 7-nm, 10-nm, and 14-nm FinFET technology nodes. These temperature variations were assumed for consumer-grade IT products following the method described in [23]. A nominal condition, V_{dd} (see Table 1) and 25°C is used as a reference condition which explains the reliability value of 100%.

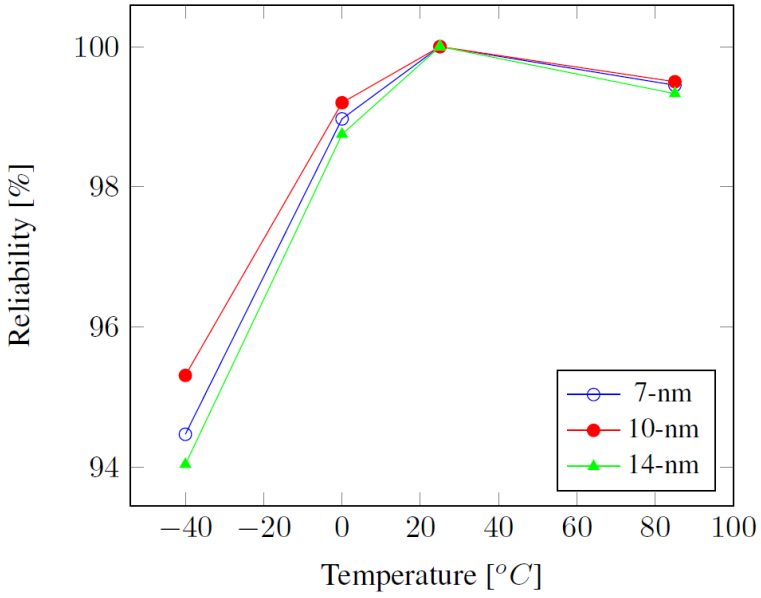


Figure 6. Reliability of 100 SRAM-PUFs subjected to temperature variations of -40°C to 85°C

By using Eq. (2) and (3), the reliability of 100 SRAM-PUFs under temperature variations of -40°C to 85°C is computed and illustrated in Figure 6. It is observed that for all three FinFET technologies, the reliability is worst at a very low temperature, -40°C which is in the range of 94% to 95%. The reliability of the SRAM-PUF response is slightly dropped at 85°C, approximately of about 98%. The impact of temperature on FinFET has been studied in [24], and the results show that V_{th} decreases as the temperature increase, while also decreasing the mobility, and vice versa. These two effects due to temperature may counteract during power-up and cause the unreliable response (i.e., bit error) of SRAM-PUF. The secret key must be free from errors to use an SRAM-PUF for cryptographic key application. The error-correction code (ECC) is required to generate a 100% reliable cryptographic key from SRAM-PUFs [6]. As the bit error rate of SRAM-PUF increases, the complexity of the ECC block increases resulted in an increase in the area overhead. This can be seen as a drawback for resource-constrained security devices. Nevertheless, from our study, the average reliability for 7-nm, 10-nm, and 14-nm FinFET technology nodes under temperature variations of -40°C to 85°C is considerably good, which is about 98% and requires a small area of ECC.

4.4 Impact of V_{dd} Ramp-up

The supply voltage ramp-up time may have an impact on the reliability of SRAM-PUF responses. The ramp-up time is defined as the required duration for the power supply circuit to achieve a desired V_{dd} value from 0V. These variations might be caused by the inefficiency of the power supply circuit. A measured response at a nominal condition, V_{dd} (see Table 1) and 25°C with ramp-up time at $1ms$ has been used as a reference condition. Other measured responses are compared against the reference condition. The ramp-up time is varied from $50us$ to $5ms$. Figure 7 portrays the reliability of SRAM-PUF responses under the ramp-up time variations at a temperature of 25°C and nominal V_{dd} for 7-nm, 10-nm, and 14-nm FinFET technology nodes. Overall, the reliability of SRAM-PUF responses under the ramp-up time variations shows no significant impact. Disregarded the noise might be one of the factors that lead to this finding [22, 25].

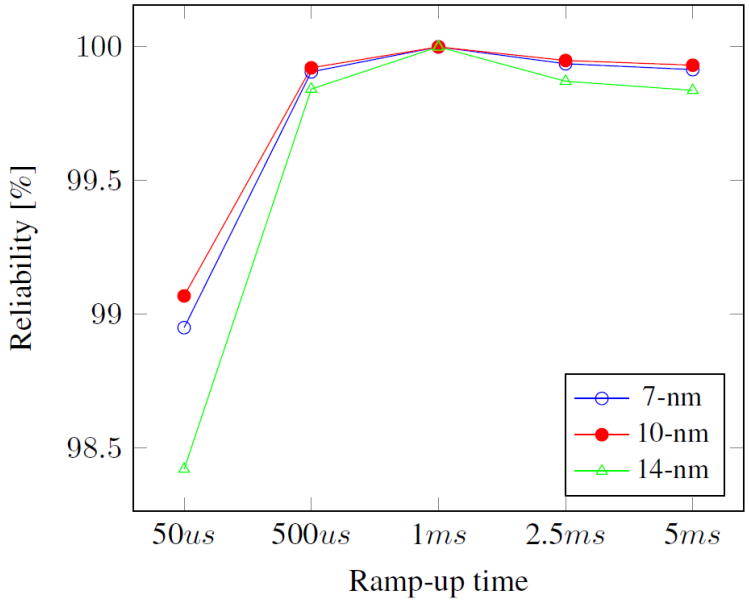


Figure 7. Reliability of 100 SRAM-PUFs subjected to different V_{dd} ramp-up time at nominal V_{dd} and 25°C temperature

4.5 Uniformity

The uniformity measures the proportion of 0's and 1's in the response bits of a PUF. A balanced number of 0's and 1's indicates the randomness in the response. Therefore, ideally, the uniformity must be distributed at 50% with a very small standard deviation, similar to the uniqueness. The uniformity is evaluated using hamming weight (HW) and it is given as:

$$Uniformity = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} r_{i,j} \times 100\% \quad (4)$$

where $r_{i,j}$ is the j-th binary bit of an n-bit response from a PUF i, for a total of m PUFs. Figure 8 depicts the uniformity distribution of 128-bit key for 100 SRAM-PUFs which were implemented using 7-nm FinFET technology, computed using Eq. (4). The value of uniformity and standard deviation for 7-nm, 10-nm, and 14-nm FinFET technology nodes are summarized in Table 4. As can be seen, the uniformity is close to an ideal value of 50%, for three different FinFET technology nodes. The small standard deviation indicates that the spread of the uniformity is centred around 50% of its mean value.

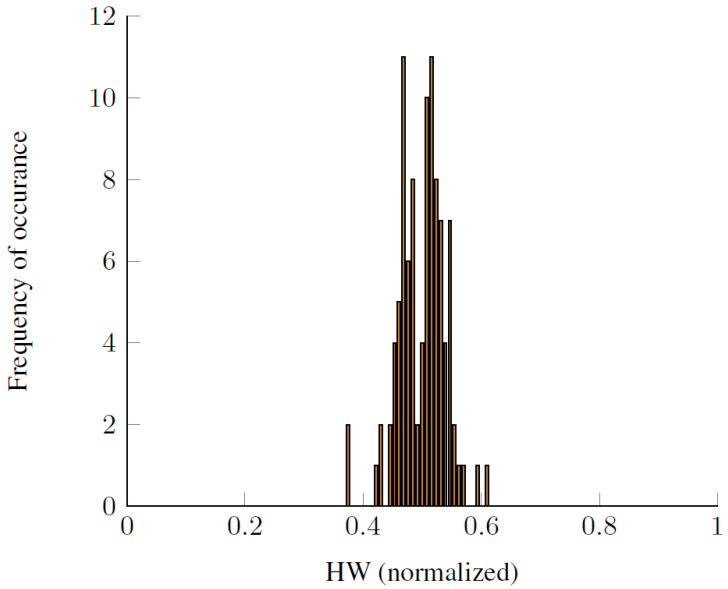


Figure 8. Uniformity of 128-bit key for 100 SRAM-PUF instances implemented using 7-nm FinFET technology node

Table 4. Uniformity

Technology	Uniformity (%)	Std. Deviation
7-nm	50.00	3.99
10-nm	50.03	3.77
14-nm	50.02	4.00

5. CONCLUSION

As the planar MOSFET reaches its scaling limit, the FinFET technology is introduced to further continue the CMOS scaling and fulfill Moore's law. In this study, the hardware security primitive, known as PUF, has been implemented using 7-nm, 10-nm, and 14-nm FinFET technology nodes, and the impact of their process variations towards the PUF performance is investigated. Our findings show that the uniqueness and uniformity of SRAM-PUF responses are distributed close to an ideal value of 50%. The average reliability of SRAM-PUF for three different FinFET technology nodes under temperature variations of -40°C to 85°C is approximately about 98%. The worst reliability is observed at -40°C, in the range of about 94% - 95%. The impact of V_{dd} ramp-up time variations is also studied. The result shows less impact on the reliability of SRAM-PUFs which might be caused by disregarding the noise. Overall, it can be concluded that 7-nm, 10-nm, and 14-nm FinFET technology nodes show no surprises on SRAM-PUF performances.

ACKNOWLEDGEMENTS

The authors would like to thank Universiti Teknikal Malaysia Melaka and the Ministry of Higher Education Malaysia for the financial funding under Grant No. FRGS/1/2020/TK0/UTEM/02/56 for completing this project.

REFERENCES

[1] M. S. Mispan, B. Halak, and M. Zwolinski, "Lightweight Obfuscation Techniques for Modeling Attacks Resistant PUFs," in IEEE International Verification and Security Workshop, (2017), pp. 19–24.

[2] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," IEEE Access, vol. **4**, (2016), pp. 61–80.

[3] M. S. Mispan, B. Halak, and M. Zwolinski, "A survey on the susceptibility of PUFs to invasive, semi-invasive and non-invasive attacks: challenges and opportunities for future directions," Journal of Circuits, Systems and Computers, vol. 30, no. 11, pp. 1–37, 2021.

[4] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in International Conference on Cryptographic Hardware and Embedded Systems, (2007), pp. 63–80.

[5] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM state as an identifying fingerprint and source of true random numbers," IEEE Transactions on Computers, vol. **58**, no. 9 (2009), pp. 1198-1210.

[6] M. S. Mispan, S. Duan, B. Halak, and M. Zwolinski, "A reliable PUF in a dual function SRAM," Integration, vol. **68**, (2019), pp. 12–21.

[7] J.W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in Symposium on VLSI Circuits Digest of Technical Papers, (2004), pp. 176–179.

[8] S. I. O'Uchi, Y. Liu, Y. Hori, T. Irisawa, H. Fuketa, Y. Morita, S. Migita, T. Mori, T. Nakagawa, J. Tsukada, H. Koike, M. Masahara, and T. Matsukawa, "Robust and compact key generator using physically unclonable function based on logic-transistor-compatible poly-crystalline-Si channel FinFET technology," in IEEE International Electron Devices Meeting, (2015), pp. 25.6.1–25.6.4.

[9] B. Narasimham, D. Reed, S. Gupta, E. T. Ogawa, Y. Zhang, and J. K. Wang, "SRAM PUF quality and reliability comparison for 28 nm planar vs. 16 nm FinFET CMOS processes," in IEEE International Reliability Physics Symposium (IRPS), (2017), pp. 2–5.

[10] M. R. Faragalla, M. A. Ewais, H. F. Ragai, M. S. Badran, and H. H. Issa, "Impact of process variability on FinFET 6T SRAM cells for physical unclonable functions (PUFs)," in International Conference on Computer Engineering and Systems, (2017), pp. 31–36.

[11] L. Zhang, C.-h. Chang, Z. H. Kong, and C. Q. Liu, "Statistical analysis and design of 6T SRAM cell for physical unclonable function with dual application modes," in IEEE International Symposium on Circuits and Systems, (2015), pp. 1410–1413.

[12] A. A. Zayed, H. H. Issa, and K. A. Shehata, "FinFET based low power ring oscillator physical unclonable functions," in International Conference on Microelectronics, (2019), pp. 227–230.

[13] H. Zhang, H. Jiang, M. R. Eaker, K. J. Lezon, B. Narasimham, N. N. Mahatme, L. W. Massengill, and B. L. Bhuva, "Evaluation on flip-flop physical unclonable functions in a 14/16-nm bulk FinFET technology," in IEEE International Reliability Physics Symposium Proceedings, (2018), pp. P–PR.1–1–P–PR.1–5.

[14] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Novel FinFET based physical unclonable functions for efficient security integration in the IoT," in IEEE International Symposium on Nanoelectronic and Information Systems Novel, (2016), pp. 172–177.

[15] E. R. Hsieh, H. W. Wang, C. H. Liu, S. S. Chung, T. P. Chen, S. A. Huang, T. J. Chen, and O. Cheng, "Embedded PUF on 14nm HKMG FinFET platform: A novel 2-bit-per-cell OTP-

based memory feasible for IoT secuirty solution in 5G era," in Symposium on VLSI Technology, (2019), pp. T118–T119.

[16] Y. H. Chang, P. S. Yeh, Y. D. Chih, J. Chang, Y. C. King, and C. J. Lin, "3D time-contingent physical unclonable function array on 16nm FinFET dielectric RRAM," in IEEE Electron Devices Technology and Manufacturing Conference, (2017), pp. 158–159.

[17] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making use of manufacturing process variations: A dopingless transistor based-puf for hardware-Assisted security," IEEE Transactions on Semiconductor Manufacturing, vol. **31**, no. 2 (2018), pp. 285–294.

[18] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel, and J. Singh, "Dopingless transistor-based hybrid oscillator arbiter physical unclonable function," in IEEE Computer Society Annual Symposium on VLSI, (2017), pp. 609–614.

[19] D. D. Lu, C. H. Lin, A. M. Niknejad, and C. Hu, "Compact modeling of variation in FinFET SRAM cells," IEEE Design and Test of Computers, vol. **27**, no. 2 (2010), pp. 44–50.

[20] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in Embedded Systems Design with FPGAs, P. Athanas, D. Pnevmatikatos, and N. Sklavos, Eds. New York: Springer New York, (2013), pp. 245–267.

[21] M. S. Mispan, M. Zwolinski, and B. Halak, "Ageing Mitigation Techniques for SRAM Memories," in Ageing of Integrated Circuits: Causes, Effects and Mitigation Techniques, B. Halak, Ed. Springer International Publishing, (2020), pp. 91–111.

[22] G. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. De Groot, V. Van Der Leest, G. J. Schrijen, M. Van Hulst, and P. Tuyls, "Evaluation of 90nm 6T-SRAM as physical unclonable function for secure key generation in wireless sensor nodes," in IEEE International Symposium on Circuits and Systems, (2011), pp. 567–570.

[23] S. Katzenbeisser, Ü. Kocaba, V. Rozic, A.-R. Sadeghi, Ingrid Verbauwhede, and C. Wachsmann, "PUFs: Myth , fact or busted? A security evaluation of Physically Unclonable Functions (PUFs) cast in Silicon," in Cryptographic Hardware and Embedded Systems – CHES 2012, E. Prouff and P. Schaumont, Eds. Springer Berlin Heidelberg, (2012), pp. 283–301.

[24] R. Saha, B. Bhowmick, and S. Baishya, "Temperature effect on RF/analog and linearity parameters in DMG FinFET," Applied Physics A: Materials Science and Processing, vol. **124**, no. 9 (2018), pp. 1–10.

[25] M. Cortez, S. Hamdioui, V. Van Der Leest, R. Maes, and G. J. Schrijen, "Adapting voltage ramp-up time for temperature noise reduction on memory-based PUFs," in IEEE International Symposium on Hardware-Oriented Security and Trust, (2013), pp. 35–40.