



Quasi-Adiabatic SRAM Based Silicon Physical Unclonable Function

Yasuhiro Takahashi¹ · Hiroki Koyasu¹ · S. Dinesh Kumar² · Himanshu Thapliyal²

Received: 16 April 2020 / Accepted: 14 July 2020 / Published online: 21 July 2020
© The Author(s) 2020

Abstract

Silicon Physical Unclonable Function (PUF) is a general hardware security primitive for security vulnerabilities. Recently, Quasi-adiabatic logic based physical unclonable function (QUALPUF) has ultra low-power dissipation; hence it is suitable to implement in low-power portable electronic devices such as radio frequency identification (RFID) and wireless sensor networks (WSN), etc. In this paper, we present a design of 4-bit QUALPUF which is based on static random access memory (SRAM) for low-power portable electronic devices and then shows the post-layout simulation and measurement results. To evaluate the uniqueness and reliability, the 4-bit QUALPUF is implemented in 0.18 μm standard CMOS process with 1.8 V supply voltage. The 4-bit QUALPUF occupies $58.7 \times 15.7 \mu\text{m}^2$ of layout area. The post-layout simulation results illustrate that the uniqueness calculated from the inter-die HDs of the 4-bit QUALPUF is 47.58%, the average reliability is 95.10%, and the energy dissipation is 29.73 fJ/cycle/bit. The functional measurement results of the fabricated chip are the same as the post-layout simulation results.

Keywords PUF · Adiabatic logic · Low-power · Hardware security

Introduction

A Physical Unclonable Function (PUF) [1] derives the hardware signature that generates from the LSI chip based on the uncontrollable process variations. These errors make the PUF response to be unique and unclonable. In the years following this introduction, an increasing number of new types of PUFs have been proposed, with a tendency towards more LSI constructions. The practical relevance of PUFs for security applications was recognized from the start, with a special focus on the promising properties of physical unclonability and tamper evidence. Silicon based PUFs have been a promising and innovative security technology; therefore

various types of PUFs such as ring-oscillator based [2, 3], SRAM based [4], bistable ring [5], etc. have been developed. In recent years, adiabatic based SRAM PUF has been first presented in [6]. This adiabatic PUF, namely, Quasi-adiabatic logic based physical unclonable function (QUALPUF) has some ultra low-power characteristics; hence it is suitable to implement in low-power portable electronic devices such as RFIDs, wireless sensor nodes, etc. However, in [6], the QUALPUF was only evaluated in security metrics including reliability, uniqueness, uniformity and bit-aliasing through SPICE simulation results.

In this paper, we present the performance of QUALPUF which is implemented in 0.18 μm standard CMOS process. From the post-layout simulation results with RC-extraction, we will show that the 4-bit QUALPUF has good uniqueness, and reliability. Then the measurement results of the fabricated LSI chip will be shown. The fabricated adiabatic PUF will be presented for the first time in the world. Through the fabricated adiabatic PUF, we will show that energy dissipation of the adiabatic PUF can be improved. The rest of the paper is organized as follows. In Section “[Related Work of PUF](#)”, we will introduce related works on PUFs. Section “[Adiabatic Switching](#)” describes the fundamentals of the adiabatic switching theory and the fundamental logic function of QUALPUF. Section “[Design of the Quasi-Adiabatic](#)

This article is part of the topical collection “Hardware-Assisted Security Solutions for Electronic Systems” guest edited by Himanshu Thapliyal, Saraju P. Mohanty, Wujie Wen and Yiran Chen.

✉ Yasuhiro Takahashi
yasut@gifu-u.ac.jp
Himanshu Thapliyal
hthapliyal@uky.edu

¹ Department of EECE, Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu 501-1193, Japan

² University of Kentucky, Lexington, KY 40506, USA

Logic Based PUF” presents the design methodology the proposed adiabatic PUF using SRAM. The simulation results and the measurement results of PUF chip are shown in Section “Simulation and Measurement Results to Experimental Results”. Then, the adiabatic PUFs are evaluated using Figure of Merit (FoM). The conclusions are summarized in Section “Conclusion”.

Related Work of PUF

The first implementation of PUF was constructed by Pappu et al. in [1]. This PUF is classified as an optical PUF based on a transparent medium, and relies on the interaction of visible light with a randomized micro-structure. These refractive particles are in random positions, sizes, and orientations due to variations in the manufacture process. However, non-electronic PUF, like an optical PUF is hard to use in the field. Because, there are the difficulty to have a tamper-resistant measuring device and the susceptibility of the responses to the alignment of the optical equipment.

The currently prevalent PUF design is the electronic PUF, such as ring-oscillator based [2, 3], SRAM based [4], bistable ring [5]. The ring-oscillator PUF is based on a delay loop (i.e., ring oscillator) to generate random bit strings. The frequency of ring-oscillator is determined by a process variation, which cannot be predicted due to manufacturing process and other uncertain factors. This kind of PUF generates the output logic-0 or logic-1 by comparing the frequencies of two circuits selected. The SRAM PUF is formed of two cross-coupled converters switch two stable states that are normally represented by 0 and 1. The behavior of an SRAM cell depends on the difference of the threshold voltages of its transistors. Even the smallest differences will be amplified and push the SRAM cell into one of two stable states. Therefore its PUF behavior is the most straightforward and most stable way to use the threshold voltages to build an identifier. The bistable PUF is the same principle of SRAM PUF, where for certain input voltage two potential arrangements of currents and voltages across the circuit are stable.

In this paper, we will design an SRAM PUF using adiabatic logic principle. Because, when the SRAM is not powered there is no key present on the chip making the solution very secure.

Adiabatic Switching

Electronic circuit-level of adiabatic switching technology was firstly presented by Younis et al. [7]. Several adiabatic logics have been proposed in the literature, e.g., [8, 9]. This section will review adiabatic switching which is

a circuit-level approach and describe adiabatic based PUF circuit, namely QUALPUF.

Theory

Energy dissipation in conventional CMOS mainly occurs during device switching. Figure 1 shows the CMOS and adiabatic switching and their working operations. When the input signal becomes high voltage, the nMOS (or pMOS) transistor goes ON state and then the load capacitance is charged by the power supply. The nMOS (or pMOS) transistor can be modeled by the effective channel resistance of the switch and the interconnect resistance. With different power supply, the CMOS and adiabatic have different current response thereby causing different energy dissipation.

In the charging operation, the supplied energy is $C_L V_{dd}^2$ while $C_L V_{dd}^2/2$ is stored energy in the load capacitance and the other $CV_{dd}^2/2$ is dissipated energy in the resistive path. During the discharging operation, the $C_L V_{dd}^2/2$ energy stored in the load capacitance is released to the ground terminal.

Adiabatic logic circuit employs AC power supply rather than the DC supply. It recovers the energy stored in the load capacitance back to the power source. In adiabatic power analysis, we will obtain the dissipated energy equation from the following equations:

$$Ri(t) + \frac{1}{C_L} \int i(t)dt = \frac{V_{dd}}{\tau} t, \tag{1}$$

where the τ is rising time of ramp voltage V_{dd} . Applying the Laplace transform and inverse Laplace transform, we have

$$i(t) = \frac{V_{dd} C_L}{\tau} \left(1 - e^{-\frac{1}{RC_L} t} \right). \tag{2}$$

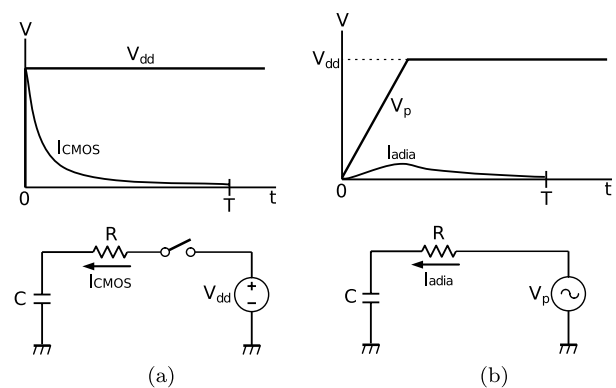


Fig. 1 RC tree model, a CMOS charging, b adiabatic charging

Energy dissipated over the period $t = 0$ to $t = \tau$ is presented as:

$$E_{\text{charge}} = \int_0^\tau p(t)dt + E(0) = R \frac{V_{\text{dd}}^2 C_L^2}{\tau^2} \left(2RC_L e^{-\frac{1}{RC_L}t} - \frac{RC_L}{2} e^{-\frac{2}{RC_L}t} - \frac{3RC_L}{2} + \tau \right) \tag{3}$$

Using the approximation of $\tau \gg RC$, the dissipated energy is equal to:

$$E_{\text{diss}} = \frac{RC_L}{\tau} C_L V_{\text{dd}}^2 \tag{4}$$

From the aforementioned equations, we can observe that the dissipated energy of the conventional CMOS depends on the value of load C_L and V_{dd} , while that of the adiabatic logic depends on switching time of τ ; hence, by increasing the time of τ , the energy dissipation of adiabatic logic is significantly lower compared to the that of CMOS logic.

Quasi-Adiabatic Logic Based PUF (QUALPUF)

This subsection reviews the quasi-adiabatic logic based PUF (QUALPUF) which was presented in [6]. Figure 2a, b show the circuit diagram of QUALPUF, and its timing chart, respectively. In the QUALPUF, the supply clock V_{pc} operates

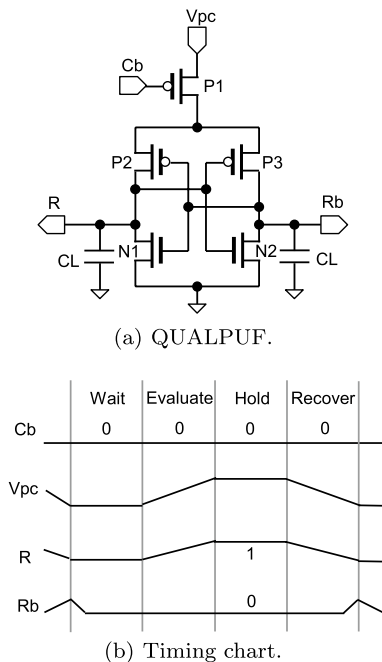


Fig. 2 QUALPUF circuit and its timing chart

in four phases: Wait, Evaluate, Hold, and Recover as shown in Fig. 2b. When the challenge bit (C_b) goes high state, the QUALPUF cell is operating in the Wait phase.

Wait

In this phase, as V_{pc} becomes 0V and C_b goes high state, the QUALPUF cell keeps a preceding state. For the pMOS (P1) to be turned ON, voltage $|V_{\text{pc}} - V_{C_b}|$ needs to be above or equal to the threshold voltage of pMOS.

Evaluate

During this phase, V_{pc} goes from 0 to V_{dd} . Drain node of P1 starts ramping from 0 to V_{dd} as transistor P1 is turned ON. When drain node of P1 reaches threshold voltage of pMOS, both P2 and P3 transistors will be conducting. The P2 and P3 will have different threshold voltage caused by the imperfections in the manufacturing CMOS process. Therefore, this leads to the flip in the outputs where one of the output leads to logic 1 and other to logic 0.

Hold

In this phase, output voltage will be hold until the recovery phase.

Recovery

In the recovery phase of the clock, the charge stored in the load capacitor is recovered back to the V_{pc} through P2 or P3 and P1 transistors.

Design of the Quasi-Adiabatic Logic Based PUF

Figure 3 illustrates a simulated 4-bit adiabatic PUF, that is a 4-bit cascaded QUALPUF. Each local PUF is queried with a single challenge bit (C_b). Each local PUF is controlled by 4 clocks where each adjacent clocks differ by a phase difference of 90° . In this adiabatic PUF, a single cell is provided four repetitive random bits. This feature of the PUF results in making it difficult for the attackers to model the PUF. For each instance of time in the local PUF, each cell is operated with a phase difference of 90° with respect to the adjacent cell. For example, if the first cell as shown in Fig. 3 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 the 4 outputs are sampled at a time leads to 4 bits. When these outputs are sampled at different phases of the clock, it leads to different pairs of bits. As a

Table 1 Simulation conditions

Power supply	1.8 V trapezoidal clock, $f_c = 100$ MHz
Transistor	0.18 μm ROHM standard CMOS process W/L = 0.6 μm /0.18 μm

result of this technique, 4 PUF cell can produce 16 bits. Figure 4 draws a layout of the 4-bit cascaded QUALPUF. The area of 4-bit QUALPUF is $58.7 \times 15.7 \mu\text{m}^2$.

Simulation and Measurement Results to Experimental Results

To analysis the performance of QUALPUF, a SPICE simulation was performed using a 0.18 μm standard CMOS process provided by ROHM corporation. Table 1 summarizes the MOS device parameters and the simulation conditions.

Figure 5 depicts a post-layout simulated output waveform of the 4-bit QUALPUF with parasitic and RC extraction. Figure 6 shows the Monte Carlo simulated output waveform of the 4-bit QUALPUF yielding a random bit with an even distribution of logic “1”s and “0”s. As the Reset signal (i.e., challenge bit Cb) is lowered, pMOS device M2 (or M3) is turned on and immediately begins to amplify the input to the comparator, which consists of an offset voltage and device noise. Discrete sampling of the mismatch and thermal noise thus occurs at low voltages. The cells that have larger mismatch evaluate faster and are less susceptible to thermal noise than those with a smaller mismatch.

From the Monte Carlo simulation results, we evaluate the uniqueness and reliability of the 4-bit adiabatic QUALPUF.

Uniqueness

The PUF uniqueness can be evaluated by the average inter-die hamming distance (HD) of the responses produced by different PUF LSI chips. The uniqueness U for m LSI chips is expressed as

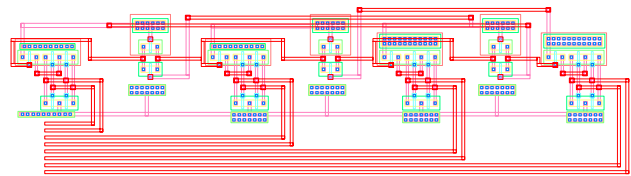


Fig. 4 Layout of 4-bit QUALPUF

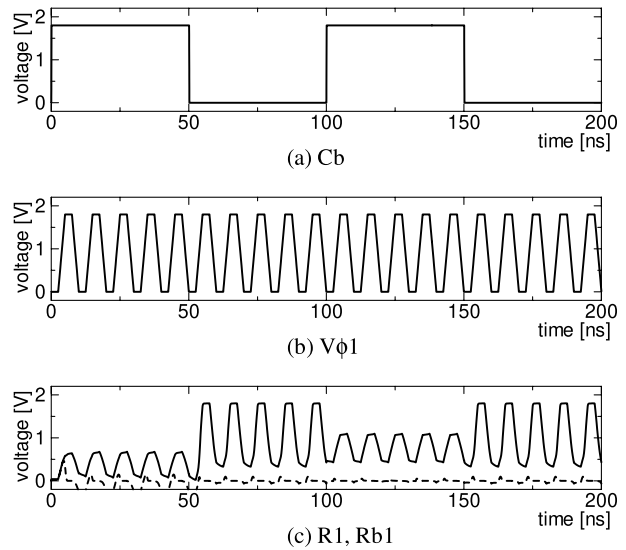
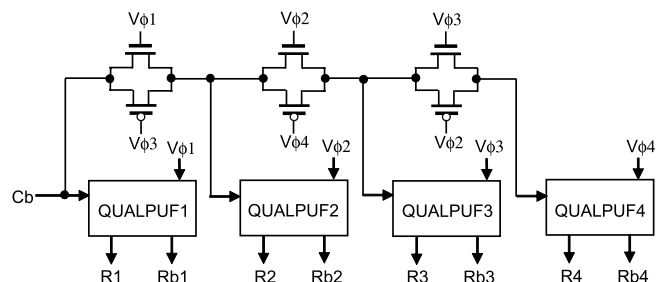


Fig. 5 Post-layout simulated output waveform of 4-bit QUALPUF

$$U = \frac{1}{m(m-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^k \frac{HD(P_i, P_j)}{n}, \tag{5}$$

where i and j are two different PUF instances, P_i and P_j are the bit numbers of the n -bit length. The ideal value of the uniqueness metric is 50%. Table 2 summarizes the uniqueness of the conventional and proposed PUFs. In this work, the uniqueness calculated from the inter-die HDs of the QUALPUF is 47.58%.

Fig. 3 Cascaded structure of 4-bit QUALPUF



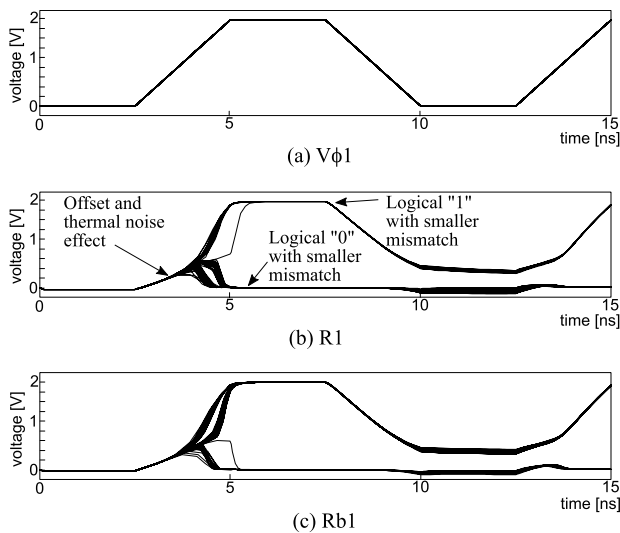


Fig. 6 Monte-Carlo simulation of 4-bit QUALPUF

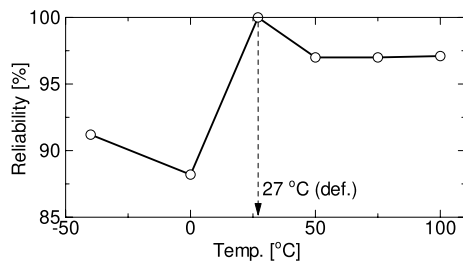


Fig. 7 Reliability of 4-bit QUALPUF against temperature variations

Reliability

The PUF reliability is used to evaluate the stability of PUF signatures generated by the same challenge in repeated experiments. The reliability can be measured by its bit error rate (BER) by comparing the responses taken at different

time with a reference response to the same challenge. The evaluation formula of reliability is

$$100 - \frac{1}{m} \sum_{j=1}^m \frac{HD(R_i, R_{i,j})}{n}, \tag{6}$$

where, m stands for the times of sampling, n is the number of bits of a signature generated by the PUF, and $R_{i,j}$ is the j -th sampling of R_i . The ideal value of the reliability is 100%. In our simulation, the working temperature is varied from -40 to 100°C , with 27°C as the reference temperature. Figure 7 shows the proposed PUF reliability with temperature variations. The proposed QUALPUF has the average reliability of 95.10% as summarized in Table 2. The post-layout simulation results show that the 4-bit QUALPUF has 29.73 fJ/cycle/bit energy consumption.

Figure of Merit (FoM)

Compared with the conventional and proposed PUFs, the Figure of Merits (FoMs) are defined as:

$$\text{FoM}_1 = \frac{\min(\text{Uniqueness}, 100 - \text{Uniqueness})}{\text{Energy} \times (\text{Area} \times \text{Process scaling})}, \tag{7}$$

$$\text{FoM}_2 = \frac{\text{Reliability}}{\text{Energy} \times (\text{Area} \times \text{Process scaling})}. \tag{8}$$

The first FoM represents the ratio between the Uniqueness and relative area-energy product. The second FoM shows the ration between the Reliability and relative area-energy product. The both FoM are lager, the performance of PUF is better. Compared with the existing fabricated PUF chip[4], our fabricated adiabatic PUF chip greatly can be improved. On the other hand, compared with Ring type PUF[3], and simulation level adiabatic PUF[6], our adiabatic PUF has the

Table 2 Comparison of conventional and proposed PUFs

PUF	Suh [2]	Su [4]	Chen [5]	Cao [3]	Kumar [6]	This work
Year	2007	2008	2011	2015	2016	2019
Topology	Ring-Osc.	SRAM	Bistable-Ring	Ring-Osc.	Adiabatic SRAM	Adiabatic SRAM
Process [nm]	90	130	n.a.	65	180	180
LSI fabrication	N (Simulation)	Y	N (Simulation)	N (Simulation)	N (Simulation)	Y
Energy [fJ/cycle/bit]	n.a.	1600	n.a.	17.5	3.9	29.73
Area [$\mu\text{m}^2/\text{bit}$]	n.a.	119	n.a.	31.3	828	230
Uniqueness [%]	46.14	64.70	50.90	50.42	40.50	47.58
Reliability [%]	99.52	96.96	98.70	97.22	96.20	95.10
FoM ₁	–	5.6×10^{-6}	–	6.5×10^{-4}	2.5×10^{-4}	1.4×10^{-4}
FoM ₂	–	3.6×10^{-6}	–	6.5×10^{-4}	2.9×10^{-4}	1.4×10^{-4}

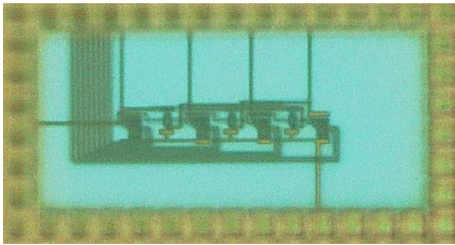


Fig. 8 Chip micro-photograph of 4-bit QUALPUF



Fig. 9 Transient waveform of 4-bit QUALPUF at 10 kHz

worst FoM; however, as well known in general, the energy dissipation of actual LSI chip increase than that of forward/back annotated simulation; the FoM of our fabricated PUF is a reasonable result considering that the LSI stands on the process rule.

Measurement Results

The 4-bit QUALPUF chip, as shown in Fig. 8 has been implemented and was evaluated as of this chip operating. Figure 9 shows the measurement results in the graph view using a digital storage oscilloscope (Rohde & Schwarz RTM3000). From this figure, we found that the correct 4-bit QUALPUF results have been outputted. After that, the outputs of 10 different IC chips were measured and then the PUF uniqueness and reliability were calculated. In the measurement results, the number of output key was set as 128-bit. The uniqueness and reliability of real QUALPUF chip are same as those of the post-layout simulation; the uniqueness is 47.58%, and the reliability is 95.10%.

Conclusion

In this paper, we reported the uniqueness and reliability of the 4-bit QUALPUF with post-layout RC extraction. From the simulation results, we found that the output of the QUALPUF is unique and unclonable. The uniqueness and reliability of QUALPUF are comparable with the existing PUFs. The functional measurement results of the fabricated chip are the same as the post-layout simulation results. The uniqueness and reliability characteristics along with low-energy consumption makes QUALPUF a promising candidate to provide hardware security in IoT devices.

The implemented adiabatic PUF has 16-bit internal state due to short length of identify key, this PUF seems to be vulnerable to attack, like a brute force attack. As to provide a more robust PUF scheme for security applications, we usually have set the 128-bit challenge sequence length or long. In near future, we will implement the 128-bit or 256-bit QUALPUF.

Acknowledgements This work was supported by VLSI Design and Educational Center (VDEC), the University of Tokyo in collaboration with Cadence Corporation and Synopsys, Inc. The VLSI chip in this study has been fabricated in the chip fabrication program of VDEC, the University of Tokyo in collaboration with ROHM Corporation and Toppan Printing Corporation.

Compliance with Ethical Standards

Conflicts of interest The authors declare that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Pappu R, Recht B, Taylor J, Gershenfeld N. Physical one-way functions. *Nature*. 2001;297:2026–30.
2. Suh GE, Devadas S. Physical unclonable functions for device authentication and secret key generation. In: *Proc. IEEE DAC 2007*, June 4–8, 2007, San Diego, CA, pp. 9–14.
3. 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(7):1143–7.

4. Su Y, Holleman J, Otis BP. A digital 1.6 pJ/bit chip identification circuit using process variations. *IEEE J Solid-State Circuits*. 2008;43(1):69–77.
5. Chen Q, Csaba G, Lugli P, Schlichtmann U, Ruhrmair U. The bistable ring PUF: a new architecture for strong physical unclonable functions. In: *Proc. IEEE HOST 2011*, June 5–6, 2011, San Diego, CA, pp. 134–141.
6. Kumar SD, Thapliyal H. QUALPUF: a novel quasi-adiabatic logic based physical unclonable function. In: *Proc. ACM CISRC 2016*, Oak Ridge, TN, pp. 1–4.
7. Younis SG, Knight TG. Asymptotically zero energy split-level charge recovery logic. In: *Proc. Napa Valley, CA: IEEE Int. Workshop Low Power Design*; 1994. pp. 177–82.
8. Kumar SD, Thapliyal H, Mohammad A, Perumalla KS. Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware. *Integr VLSI J*. 2017;58:369–77.
9. Koyasu H, Takahashi Y. Current pass optimized symmetric pass gate adiabatic logic for cryptographic circuits. *IPSI Trans Syst LSI Des Methodol*. 2019;12:50–2.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.