

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,000

Open access books available

148,000

International authors and editors

185M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Low-Power CMOS/FinFETs Circuit Using Adiabatic Switching Principle

Cancio Monteiro

Abstract

Power consumption has become a very serious concern with regard to the rapid technology of Internet of Things (IoT) devices. The IoT devices, such as sensor nodes, secure cryptographic devices, and medical implantable devices are general embedded systems that require low power and operate at low-frequency speed. Countless efforts have been done to reduce power consumption in complementary metal oxide semiconductors (CMOS) through supply voltage downscaling, reducing unnecessary clock activity, avoiding long path circuit topology, etc. Another circuit technique for low-power purpose is by employing adiabatic switching principle. The adiabatic switching is commonly used in minimizing energy loss during charging/discharging period at all nodes of the circuit. In this paper, a low-power adiabatic CMOS/FinFETs circuit for low-power secure logic application is presented. The circuit speed, power consumption, and other evaluation metrics indicating the circuit performances will be compared among the proposed circuits and other circuit topologies that are available in the literature.

Keywords: CMOS, adiabatic, low-power, FinFETs, dual-rail, PUF, secure logic, LSI multiplier

1. Introduction

In recent years, the emerging Internet of Things (IoT) technology has introduced challenges and opportunities for engineering-related fields. It is estimated that the number of active IoT devices will surpass 25.4 billion in 2030 [1], including wired and wireless sensor networks. Most researchers consider the security profile (authenticity, integrity, and confidentiality) [2–8] and power-saving crypto-devices [9, 10] as challenging efforts in IoT network design for resilient and sustainable infrastructure of Industry 4.0 [11]. With the rapid growth of portable and standalone IoT devices, the energy availability has to be well-managed to assure the sustainability of IoT connectivity. These IoT devices can be supplied either by utilizing abundant ambient energy sources [12] or by powering with rechargeable battery technology. In this context, the electronic circuit design technique that is able to consume low power has to be addressed. To contribute to the secure communication among IoT devices, the circuit designers are again demanded to produce secure cryptographic devices to withstand

side-channel-analysis (SCA) attract techniques [13–16]. In tackling both the low-power and high-security demand, numerous efforts have been done at the circuit design level by employing the adiabatic switching principle [17]; such as secure adiabatic logic (SAL) [18], symmetric adiabatic logic (SyAL) [19], 2N-2N2P [20, 21], charge-sharing symmetric adiabatic logic (CSSAL) [22], 2-phase symmetric pass gate adiabatic logic (2-SPGAL) [23], and the secure quasi-adiabatic logic (SQAL) [24]. Moreover, to confirm the authenticity of any crypto-device, a physically unclonable function (PUF) circuit is utilized to verify the chip authenticity and for secure key generation [25, 26]. Definition of a PUF in [27] states that a PUF is a hardware security fundamental that translates an input challenge into an output response through a physical system in a manner that is specific to the exact hardware instance (unique) and cannot be replicated (unclonable). The PUF related SRAM-based circuit design in adiabatic operation was first reported in Quasi-Adiabatic Logic PUF (QUAL-PUF) [28]. Accordingly, the author of this paper then proposed the CMOS-based two-phase clocking adiabatic PUF (TPCA-PUF) [29], and the PUF circuit stability is further investigated under various temperature and process variations using FinFETS technology [30].

In this paper, the author further describes the adiabatic circuit design technique for low-power application, using single-rail and dual-rail circuit topologies. The proposed circuits' operation, the evaluation metrics utilized for secure logic verification, the frequency spectrum of the proposed circuits, and the LSI circuit design using proposed circuits in comparison with previous works to validate the effectiveness and the performances of the proposed works are presented.

The rest of this paper is structured as follows: Section 2 describes the fundamental low-power circuit design, which briefly describes the adiabatic switching principles in comparison with the conventional CMOS logic circuit. Section 3 presents the proposed CMOS logic circuit topologies in detail. Section 4 describes the proposed LSI circuits, their respective simulation conditions, and the security evaluation metrics. Simulation results and technical discussion of the proposed works in comparison with the convention-related circuits are discussed in section 5. Finally, Section 6 concludes the research findings of this work.

2. Low-power circuit design technique

To ensure the long battery life for battery-powered embedded cryptographic devices, the CMOS power consumption needs to be highly considered. There have been several circuit design techniques reported to reduce dynamic power consumption, such as reducing supply voltage to near and subthreshold regions, reducing circuit switching activities, and avoiding long critical paths to diminish unnecessary glitch current, etc. From the circuit supply voltage point of view, adiabatic logic principle is a promising technique that can guarantee the efficiency of power usage. Therefore, in the following subsections, the author describes power consumption comparison among conventional and adiabatic CMOS logic styles.

2.1 Power consumption of CMOS circuit

Total power in a CMOS circuit comes from dynamic power, short-circuit power, and static (or leakage) power, as indicated in **Figure 1**. The dynamic power consumption occurs when the output node's capacitor C_L is switched (charging period).

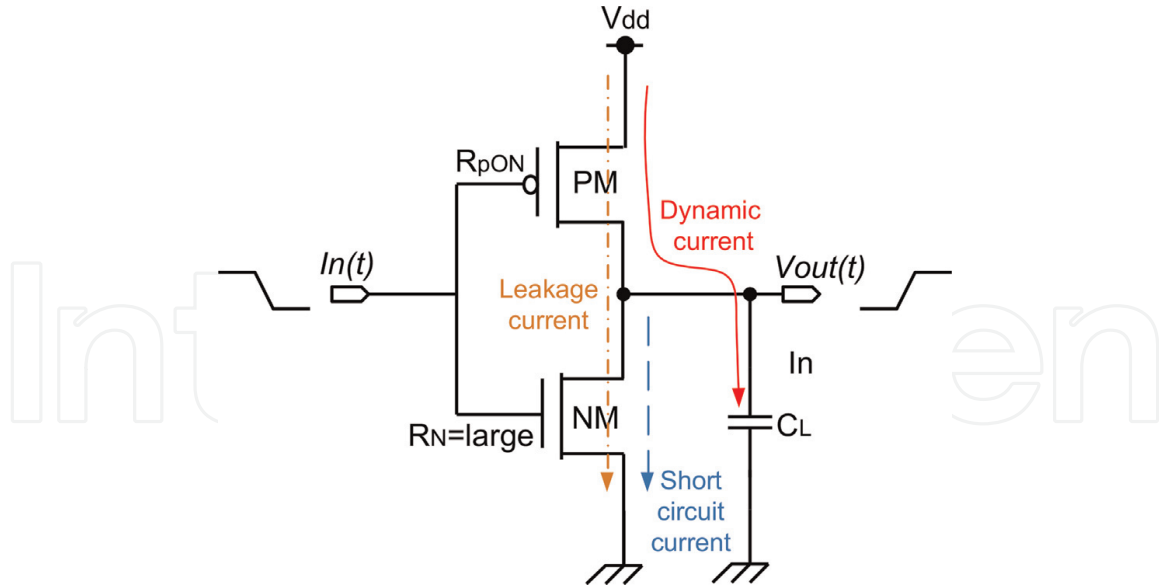


Figure 1.
 Total power-on CMOS inverter: Dynamic Power, short-circuit power, and the leakage power.

The short-circuit power happens when both PMOS (PM) and NMOS (NM) transistors operate simultaneously during a short period of time of different input signal transitions (such as $In(t)$ signal changes from $0 \rightarrow 1$ and $1 \rightarrow 0$). The other contributing power is the static power, which is consumed at either PM or NM transistor that operate in the cutoff region (or any electronic device is in standby mode).

$$P_{Total} = P_{Dynamic} + P_{SC} + P_{Static} \quad (1)$$

2.1.1 Dynamic power

Dynamic power consumption commonly depends on the switching frequency f , amplitude of power supply V_{dd} , and the load capacitance C_L of the output node. The operation of CMOS inverter logic in **Figure 1** is that when the state of input signal $In(t)$ changes from $1 \rightarrow 0$, the PM transistor is switched ON, and the current supply from V_{dd} is flowing down to charge the output node of C_L from initial condition of $V_y(0_-) = 0 \rightarrow V_y = V_{dd}$. The internal equivalent RC model during this operation is called a pull-up network (PUN), as shown in **Figure 2a**. On the other hand, when the state of input signal $In(t)$ changes from $0 \rightarrow 1$, the NM transistor is switched ON and the output node of V_y is discharged from initial condition of $V_y(0_-) = V_{dd} \rightarrow V_y = 0$ level (grounded). The internal equivalent RC model during this operation is called a pull-down network (PDN), as shown in **Figure 2b**.

From **Figure 2**, the total power dissipation can be calculated using each network system. By considering the MOS resistance value of $1/gm_n = 1/gm_p = R$, $C_L = C$, we can calculate the current source that flows into the circuit, as shown in Eq. (2):

$$ip(t) = i(t) = \frac{V_{dd}}{R} e^{-\frac{t}{RC}} \quad (2)$$

The power consumption is calculated as:

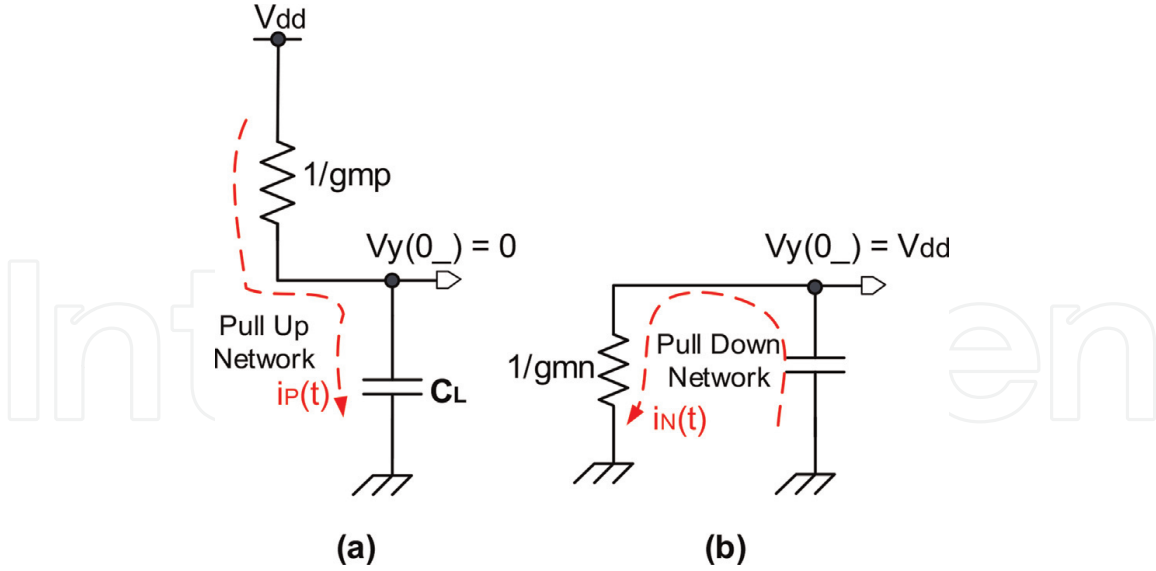


Figure 2. (a) A CMOS pull-up network (PUN) RC equivalent model for charging phase, (b) A CMOS pull-down network (PDN) RC equivalent model for discharging phase.

$$p(t) = i(t)V_R(t) = i(t)^2 R = \frac{V_{dd}^2}{R} e^{-2\frac{1}{RC}t} \quad (3)$$

Hence, the energy dissipated over the period of $t=0$ to $t=\tau$ is calculated as follows:

$$E_{charge} = \int_0^\tau p(t)dt = \int_0^\tau \frac{V_{dd}^2}{R} e^{-2\frac{1}{RC}t} dt = C \frac{V_{dd}^2}{2} \left(e^{-2\frac{1}{RC}\tau} + 1 \right), \quad (4)$$

If, $\tau \gg RC$, then the energy charged in output load capacitance is:

$$E_{charge} = \frac{1}{2} CV_{dd}^2 \quad (5)$$

From Eq. (5), half of the energy is dissipated as heat by the resistance $1/g_{mp}$ in **Figure 2a**; therefore, the total energy dissipated from power supply during PUN operation is $E_{total} = CV_{dd}^2$. Then, the average dynamic power $P_{dynamic} = E_{total}/T$, which is consumed during a certain period of time T can be formulated as

$$P_{dynamic} = \alpha f CV_{dd}^2, \quad (6)$$

where, the f denotes the clock frequency, and α is the switching activity factor, which corresponds to the average number of $0 \rightarrow 1$ transitions that occur at the output cell in each clock cycle.

2.1.2 Short-circuit power

Short circuit power (P_{SC}) usually occurs because there is no zero second exist during different data transitions in CMOS logic circuit. The detailed discussion of short-circuit power was reported in [31], with an expression shown in Eq. (7);

$$P_{SC} = \frac{1}{12} \beta \tau f (V_{dd} - 2V_T)^3 \quad (7)$$

where β is a gain factor of a MOS transistor, τ represents the rise and fall time, f denotes a clock frequency, and the V_T is the MOS transistor threshold voltage.

2.1.3 Static power

Static power consumption is power loss when the transistor is not in the process of switching (cut-off state). It occurs when a small leakage current (I_{leak}) is flowing through the MOS transistor that is turned off. Static power is increasing significantly proportional to the shrinking of CMOS process technology.

There are several components that trigger the occurrence of leakage power [32, 33] as shown in **Figure 3**; such as (1) Reverse bias diode leakage current (I_{rbd}), which occurs due to the reverse bias current of p-n junction between diffusion region of the transistor and substrate; (2) Gate oxide tunneling current (I_{ox}) is the leak current that flows from oxide insulation to substrate; (3) Gate induced drain leakage ($GIDL$) is another leakage current that increases exponentially due to the reduced gate oxide thickness; and (4) Subthreshold leakage current (I_{sub}). Thereby, the total summation of all leakage current I_{leak} components aforementioned can be formulated as:

$$P_{leak} = I_{leak} V_{dd} \quad (8)$$

2.2 Adiabatic switching principle

The adiabatic switching technique enables the logic circuit to reuse energy stored in output load capacitance during the recovery phase, known as energy recycling [17]. For better understanding of the adiabatic switching principle, the author uses the same RC model circuit with a different power supply as depicted in **Figure 4**. **Figure 4a** represents conventional logic with constant step V_{dd} voltage, whereas **Figure 4b** explains the concept of adiabatic switching with ramped step voltage, which is defined by the length of time.

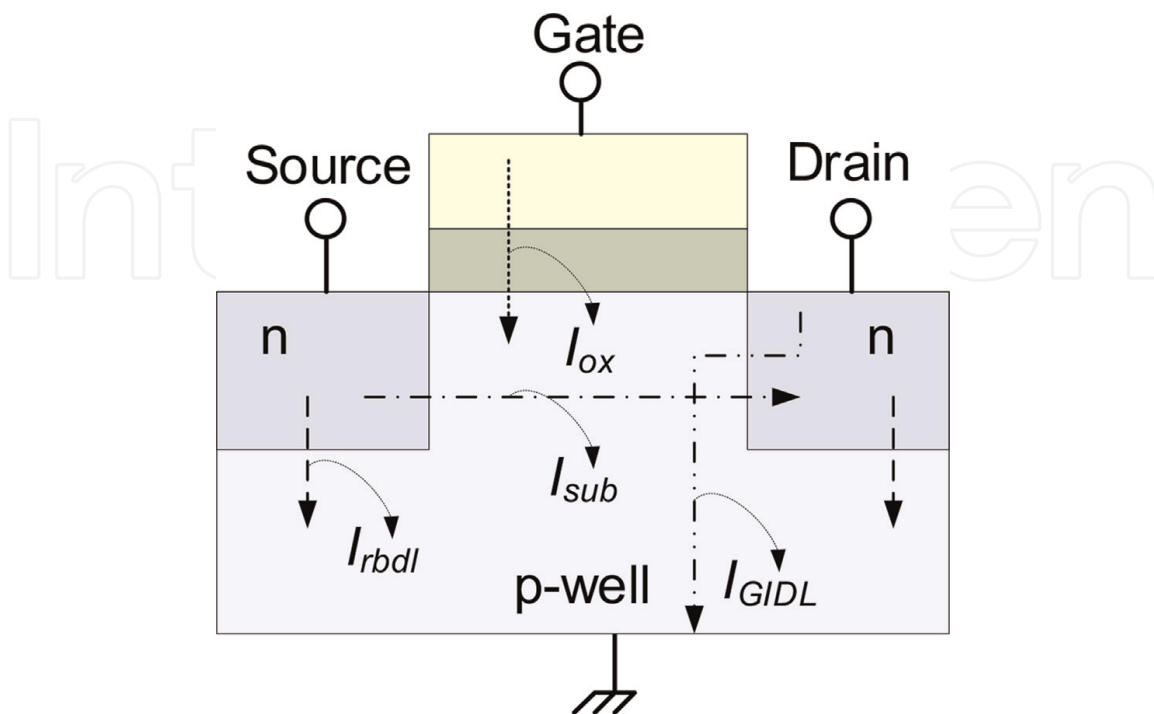


Figure 3. Components of leakage power in CMOS [34].

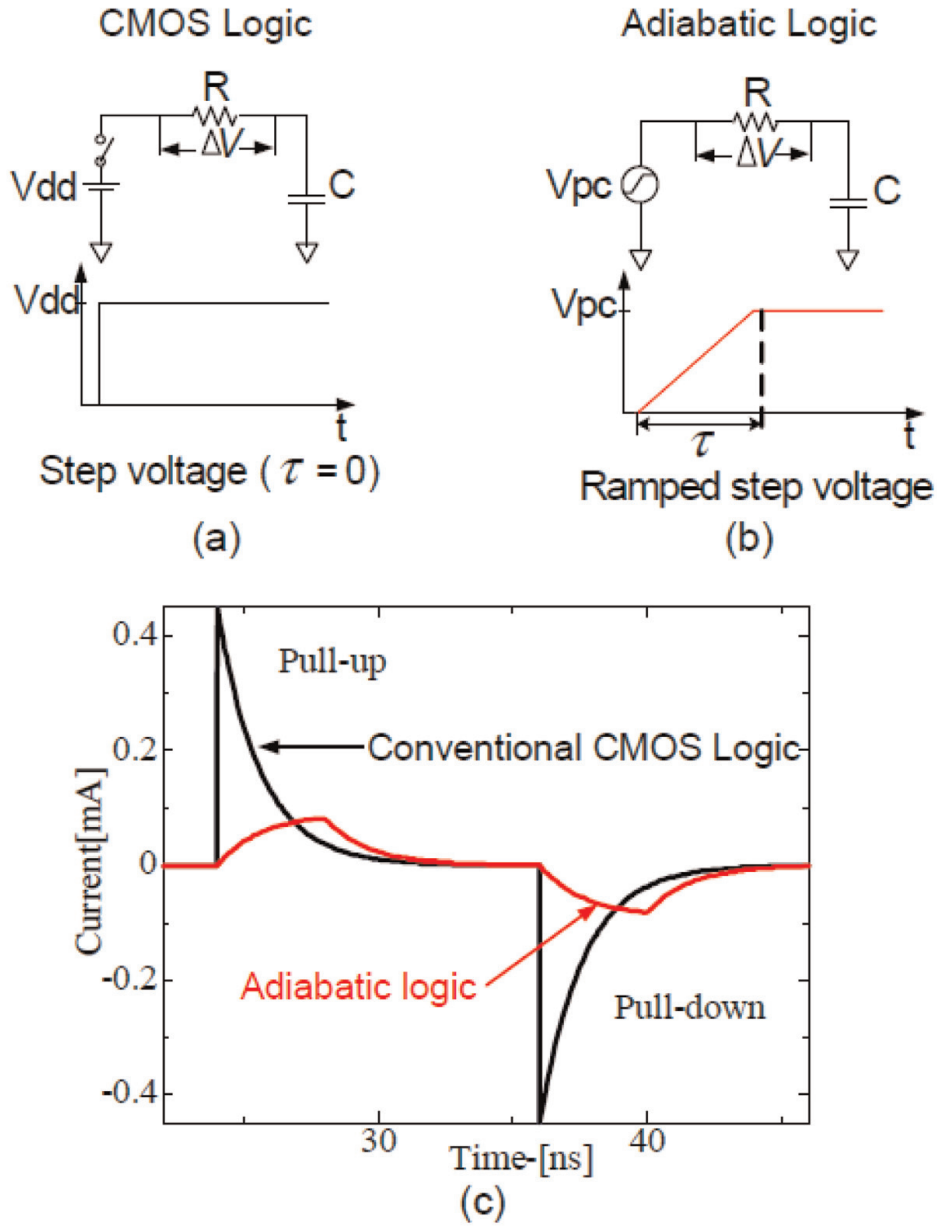


Figure 4. Equivalent RC model of CMOS logic versus adiabatic logic; (a) CMOS logic with step voltage and (b) Adiabatic logic with ramped step voltage. (c) The peak supply current of the adiabatic logic is significantly lower than that of the conventional CMOS logic under the same simulation parameters and conditions.

Applying Kirchhoff Voltage Law (KVL) for the circuit in **Figure 1a** and **b**, the equation for charging network of the conventional CMOS is expressed in Eq. (9)

$$R_{i(t)} + \frac{1}{C} \int_0^T i(t)dt + v(0_-) = V_{dd} \quad (9)$$

and the charging network for adiabatic switching is similarly expressed in Eq. (10)

$$R_{i(t)} + \frac{1}{C} \int_0^T i(t)dt + v(0_-) = \frac{V_{dd}}{\tau}(t) \quad (10)$$

where τ is the rising time of ramp voltage V_{dd} . Applying the Laplace transform and inverse Laplace transform, we obtain the charging current as expressed in equations (11, 12) for CMOS logic and adiabatic logic, respectively:

$$i(t) = \frac{V_{dd}}{R} e^{-\frac{1}{RC}t} \quad (11)$$

$$i(t) = \frac{V_{dd}C}{\tau} \left(1 - e^{-\frac{1}{RC}t}\right) \quad (12)$$

The peak current difference of (Eqs. 11, 12) shows a large area and sudden flow of the current of the conventional CMOS, and gradual increase of supply current peak of the adiabatic switching in accordance with slow rising τ , which can be observed in **Figure 1c**.

Further analysis from an energy consumption perspective, the dissipated energy over the period $t = 0$ to $t = \tau$ is expressed as in Eq. (13)

$$E_{diss} = \int_0^{\tau} Ri^2(t)dt + E(0_-) \quad (13)$$

Substituting current $i(t)$ in Eqs. (11, 12) into Eq. (13), we have energy stored in capacitance for each conventional CMOS and adiabatic switching as expressed in Eqs. (14, 15), respectively.

$$E_{CMOS} = \frac{1}{2} CV_{dd}^2 \quad (14)$$

$$E_{Adiabatic} = \frac{RC}{\tau} CV_{dd}^2 \quad (15)$$

Eq. (15) obviously shows that by increasing the time of τ , the energy dissipation of adiabatic logic is significantly lower compared to the one of the conventional CMOS logics in Eq. (14).

3. CMOS logic circuit topology

The logic circuit available in the literature has two kinds of circuit topologies; the single-rail (SR) logic circuit composes of static CMOS (scCMOS: see **Figure 1**) and dynamic CMOS logics [35], and the dual-rail CMOS logic (DR-CMOS or differential logic) [20, 36], as depicted in **Figures 5a** and **b**. Regarding these circuits, uncountable research have been done from the viewpoint of low-power dissipation [20, 36–41], high speed, and further application into the secure cryptographic hardware design [18–24, 42, 43]. From the logic's security perspective, balancing supply current flows into the circuit is the main constraint, since the side-channel cryptanalysis targeting for the different peak current/power traces when crypto devices execute encryption and decryption processes [14]. Hence, **Figure 5** describes the supply current traces at different input data transitions for conventional static CMOS, dual-rail CMOS circuits (refers to **Figure 5a** and **b**, respectively), and our previously proposed charge-sharing symmetric adiabatic logic (CSSAL [22]). Effective side-channel analysis countermeasure is how the circuit is able to mask different input transitions with the same supply peak current despite any input–output data flipping. This can be solved by the charge-sharing technique of the proposed CSSAL circuit. In addition, the CSSAL adopted the adiabatic switching principle, which lower peak current compared with the conventional CMOS logic technique in scCMOS and DR-CMOS in **Figure 5**.

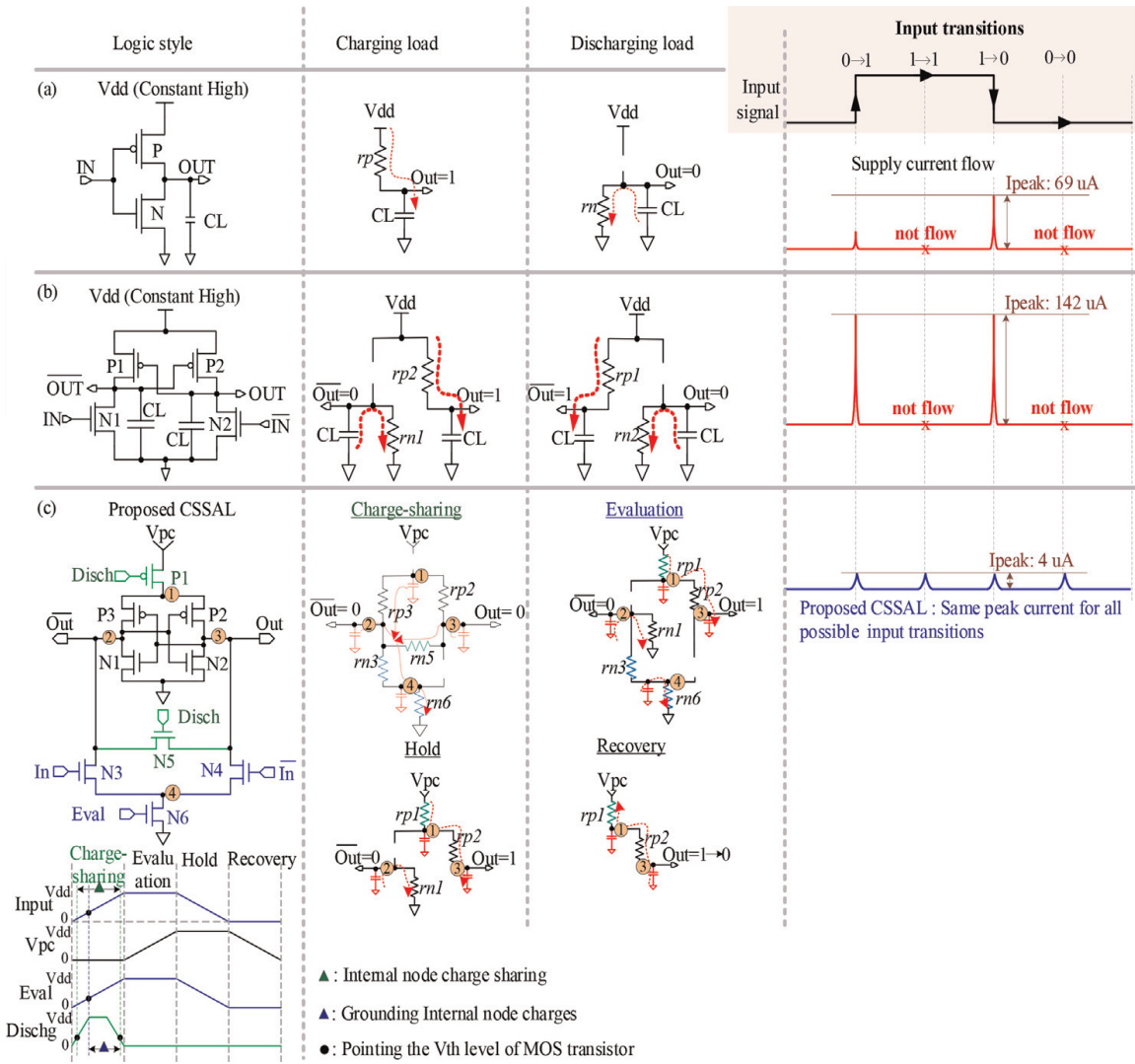


Figure 5. Logic circuit topology and each of its supply current traces.

4. Proposed LSI circuit

The author of this paper has proposed three different circuit applications based on SR and DR CMOS circuit topologies for low-power and high-security profile, such as CSSAL [22], the source biased semi-adiabatic logic (SBSAL) [41], and the two-phase clocking adiabatic physical unclonable function (TPCA-PUF) [29]. In these following sub-sections, the author will present the fundamental circuit topology of each and their respective LSI block diagram.

4.1 The CSSAL circuit

The fundamental inverter logic style of the CSSAL circuit is shown in **Figure 5c**. The CSSAL is designed using DR circuit topology with four phases of adiabatic switching operations (charge-sharing, evaluation, hold, and recovery phases) [22], in which, the same internal equivalent RC model of each phase occurs for all possible different input data transitions, which yielding the same peak current as depicted in the right side of **Figure 5c**. It is obviously shown in **Figure 5** that the CSSAL performs balanced low peak current in comparison with the other logic circuits along the four

different input transitions. This type of supply current trace is difficult to predict the position of its true input data, hence it is secure and applicable for cryptographic LSI design (**Figure 6**). To validate the security merit of the proposed CSSAL, the bit parallel cellular multiplier over finite field $GF(2^4)$ has been designed and implemented using the 0.18 μm CMOS process technology. Input-output signals of the bit parallel cellular multiplier over $GF(2^4)$ are depicted in **Figure 7**.

4.2 The SBSAL circuit

The proposed SBSAL circuit is a type of SR static CMOS logic family in adiabatic switching operation with sinusoidal power clock supply, as depicted in **Figure 8d**. The SBSAL circuit is basically operated in charging and discharging periods, in which the equivalent RC model of PUN and PDN are depicted in **Figure 9a** and **b**. This figure illustrates the output voltages, the instantaneous power, and the energy dissipated during charging and discharging phases. The total energy loss in SBSAL logic circuit is formulated in Eq. (16) as follows:

$$E_{\text{SBSAL}} = \frac{RC}{\tau} CV_{\text{PC}}^2 + \frac{1}{2} CV_{\text{bias}}^2 + \frac{RC}{\tau} C(V_{\text{out}} - V_{\text{bias}})^2 \quad (16)$$

This Eq. (16) means the energy stored in the load capacitance C_L is recycled to V_{bias} power supply. Although there is nonadiabatic energy loss of $\frac{1}{2} CV_{\text{bias}}^2$ in Eq. (8), the V_{bias} is set to 0.23 V, which has very low contribution to the total energy loss in the circuit. The SBSAL circuit PDN network is connected to 0.23 Volt bias voltage instead of connecting to ground or another sinusoidal supply voltage. This connection technique will only require one circuit to produce V_{pc} power supply. This means that the proposed SBSAL has low complexity if compared to the other adiabatic logic family shown in **Figure 8b** and **c**.

To validate the effectiveness of the proposed logic as a low-power SBSAL circuit, we implemented a 4x4-bit array SBSAL LSI multiplier as depicted in **Figure 10**. It is verified that the SBSAL multiplier logic function is well operated as shown in **Figure 11**.

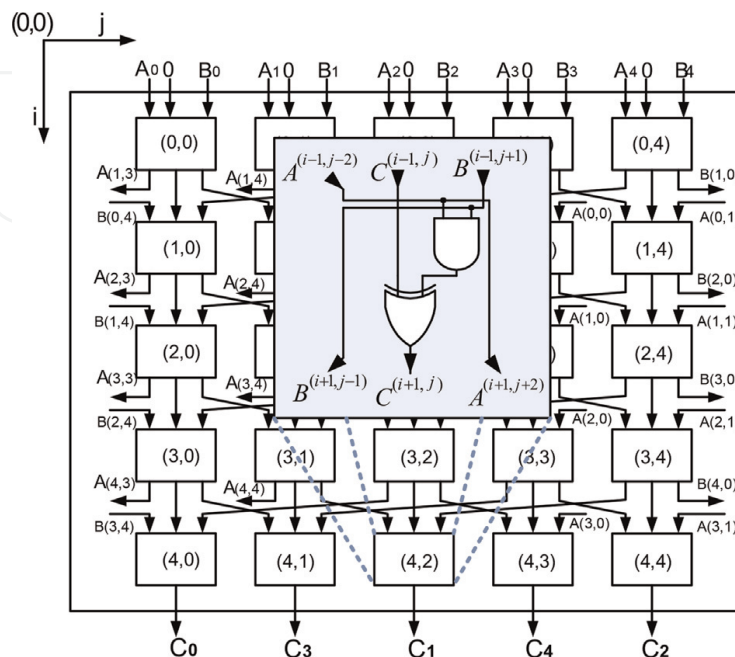


Figure 6.
 The circuit block diagram of the bit parallel cellular multiplier over $GF(2^4)$.

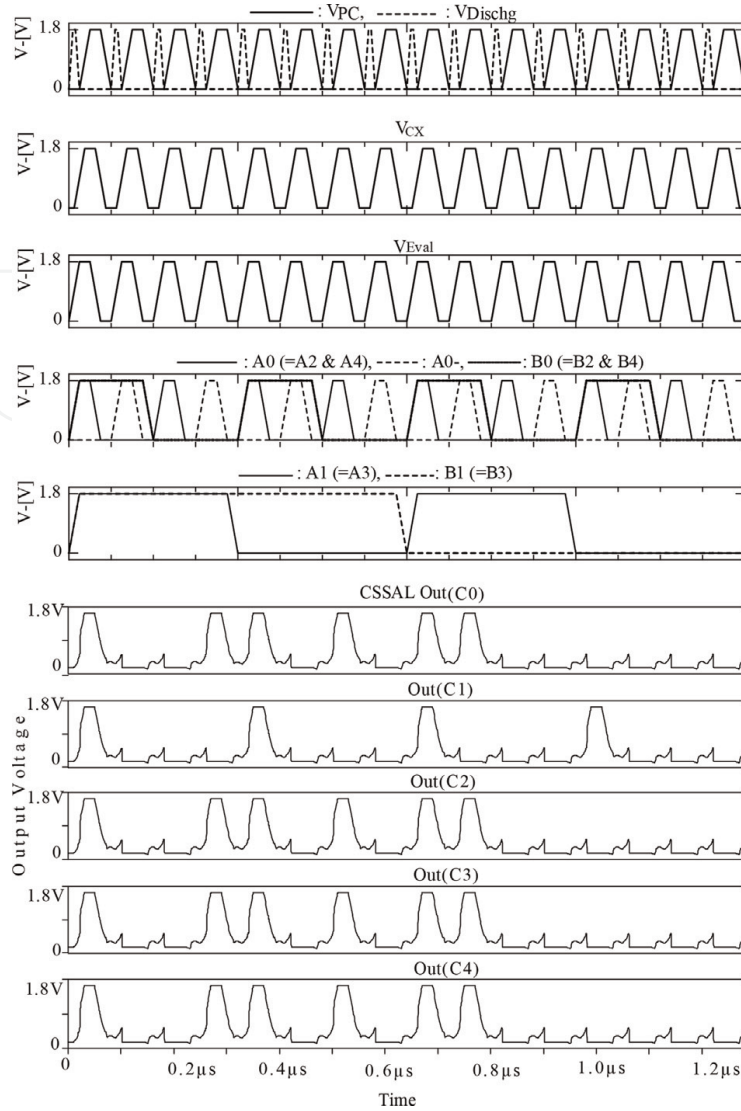


Figure 7. Input-Output signals of the CSSAL bit parallel cellular multiplier over $GF(2^4)$.

4.3 The TCPA-PUF circuit

The proposed adiabatic FinFETs based PUF circuit topology is depicted in **Figures 12 and 13a**. It was designed with cross-coupled latch circuit based on SRAM circuit topology. The challenge signal of the proposed PUF circuit is controlled by the static CMOS inverter aimed to conduct charging and discharging of the PUF cell semi-adiabatically using a trapezoidal power clock signal of V_{pc} . Notable improvement from QUAL-PUF circuit topology, the TCPA-PUF controls the current flow from output nodes to slowly flow to the ground through N4 transistor by controlling its operation speed with a ramped V_{pc-} signal. Notably, in the proposed adiabatic PUF circuit, the author applies two phases of power clock signals V_{pc} and V_{pc-} , as depicted in **Figure 14b**. The circuit operation of the TCPA-PUF cell is shown in **Figure 15**. Detailed TCPA-PUF circuit operation in an adiabatic mode for CMOS-based design has been clearly explained in [29], and the FinFETs-based TCPA-PUF design can be accessed in [30].

To verify the effectiveness and the stability of the proposed SRAM based TCPA-PUF, the author designs a 4-bit cascaded adiabatic PUF as depicted in **Figure 14**. Each local PUF is supplied with four different power clocks with a phase difference of 90° .

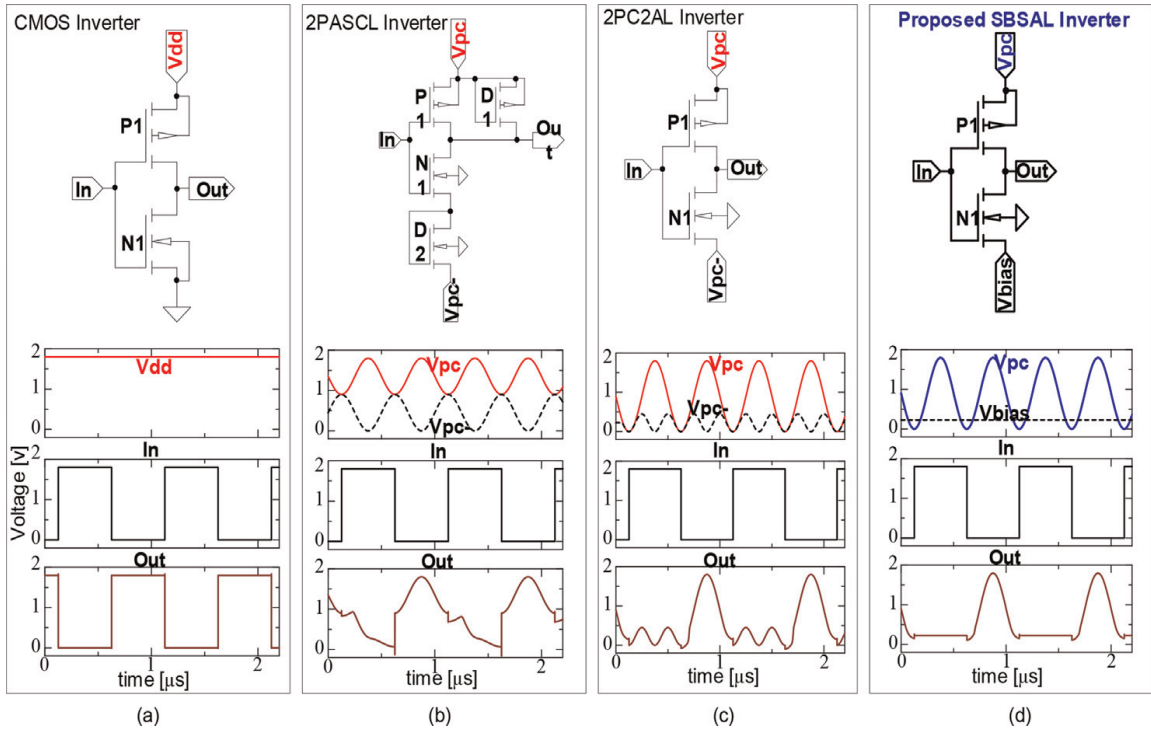


Figure 8. Inverter logic investigated; a) Conventional CMOS logic, b) Adiabatic 2PASCL logic [39], c) Adiabatic 2PC2AL logic [40], and d) Proposed SBSAL [41].

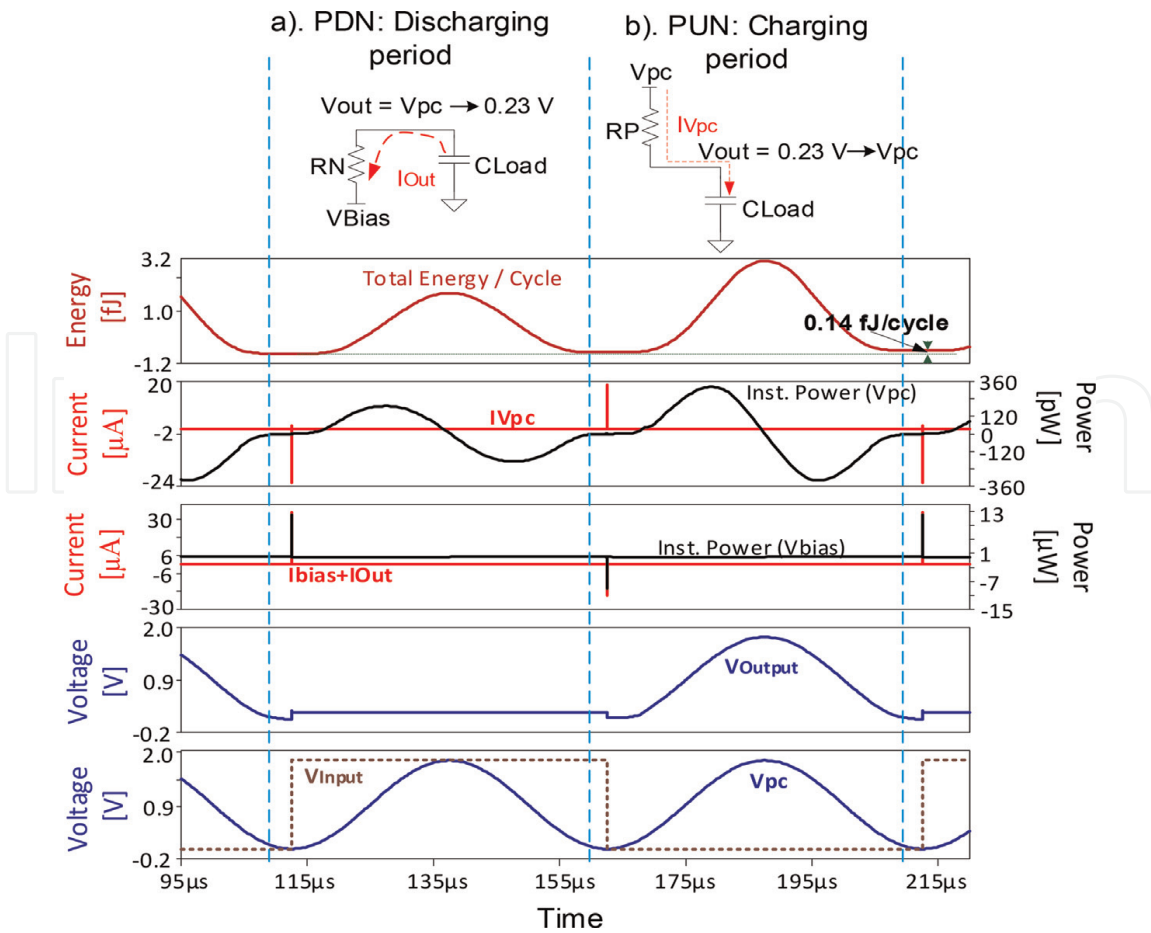


Figure 9. Proposed SBSAL logic operation; a) Discharging period and b) Charging Period.

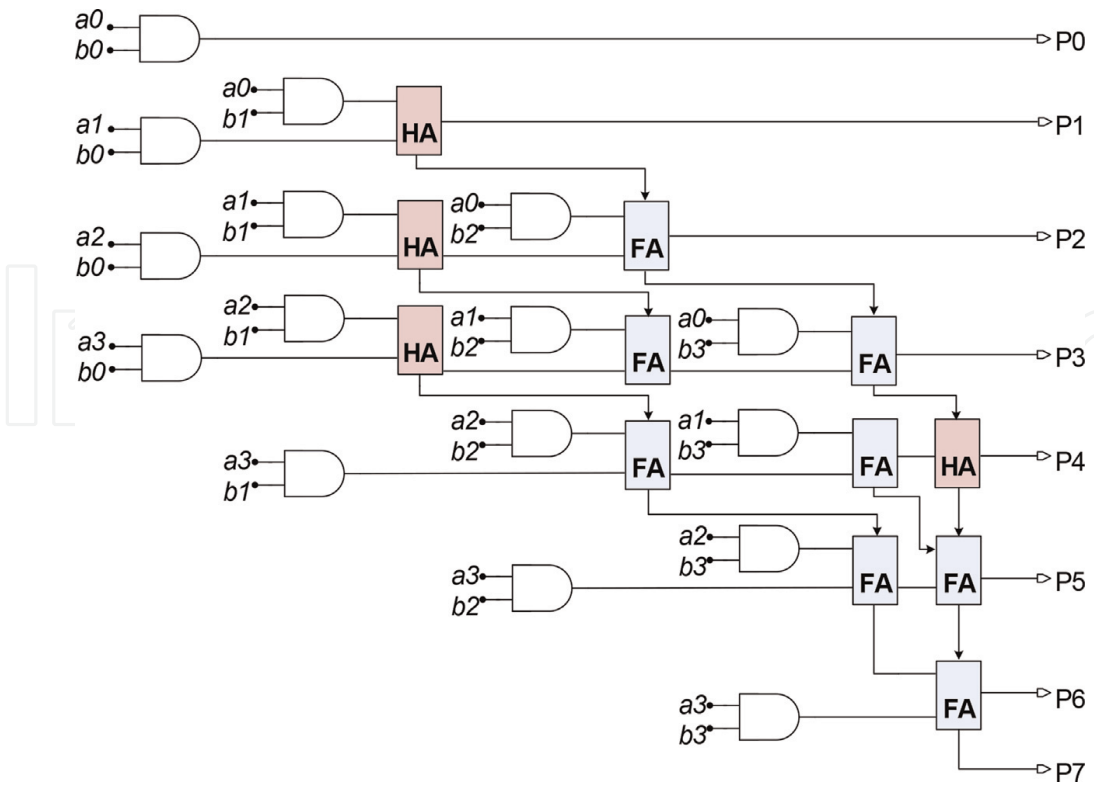


Figure 10.
Circuit diagram of a 4x4-bit array LSI multiplier.

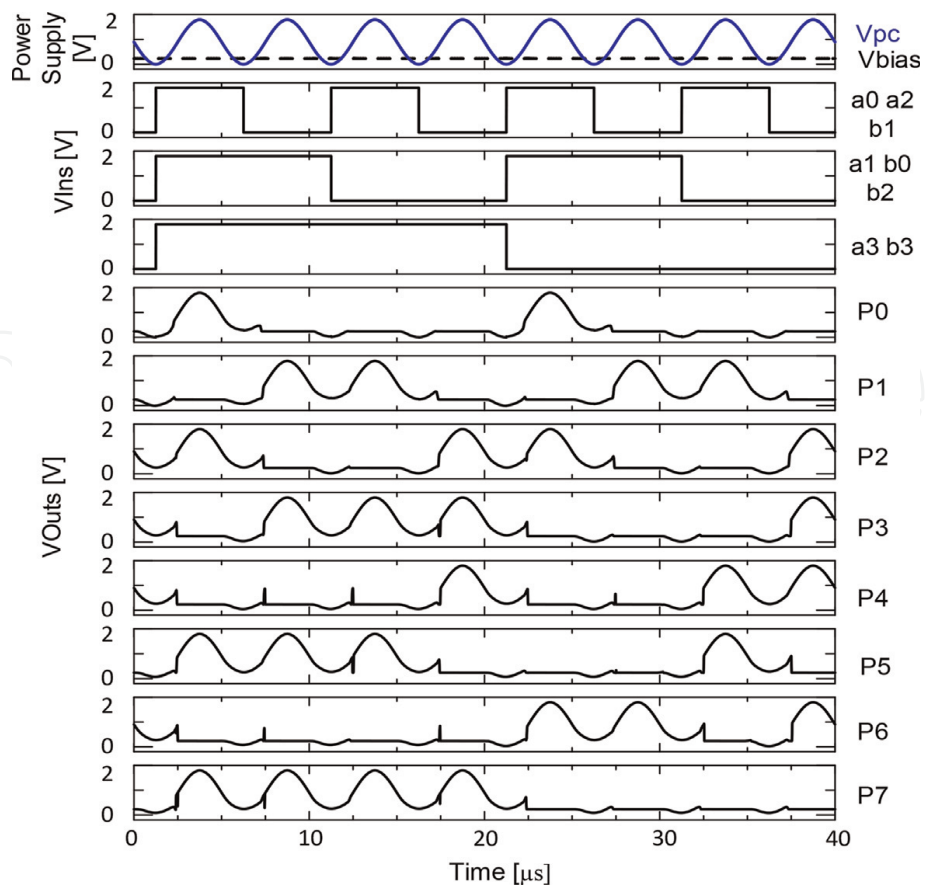


Figure 11.
Input-output signals of SBSAL multiplier at 25 MHz.

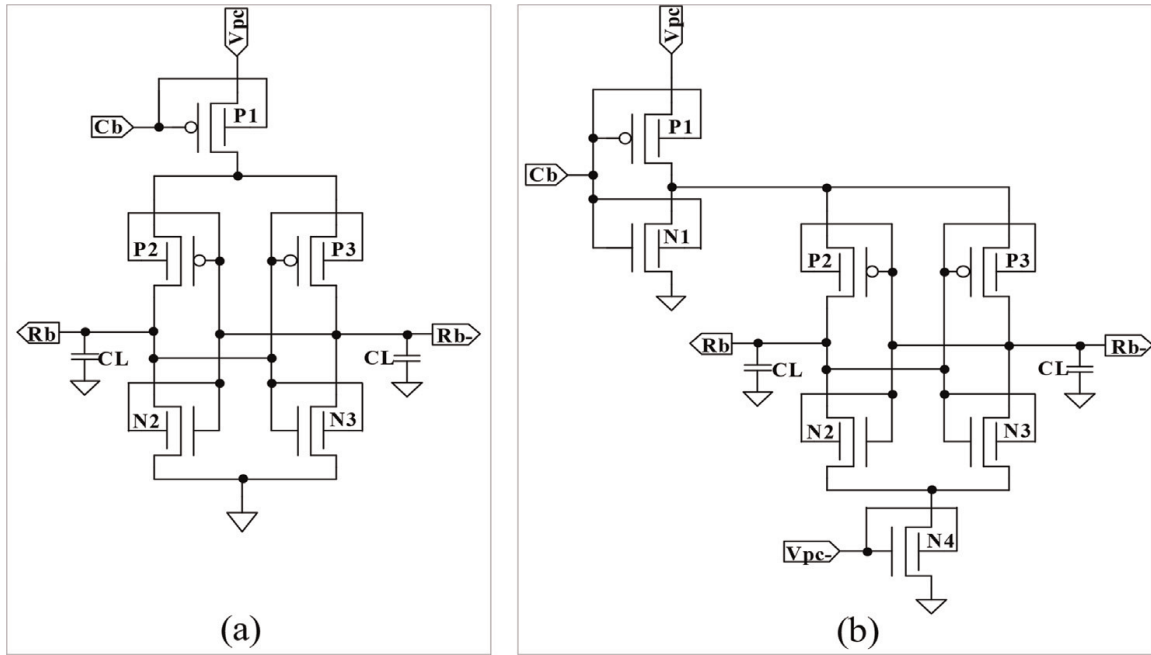


Figure 12. SRAM-based FinFET PUF circuit; (a) QUAL-PUF circuit, (b) TCPA-PUF circuit.

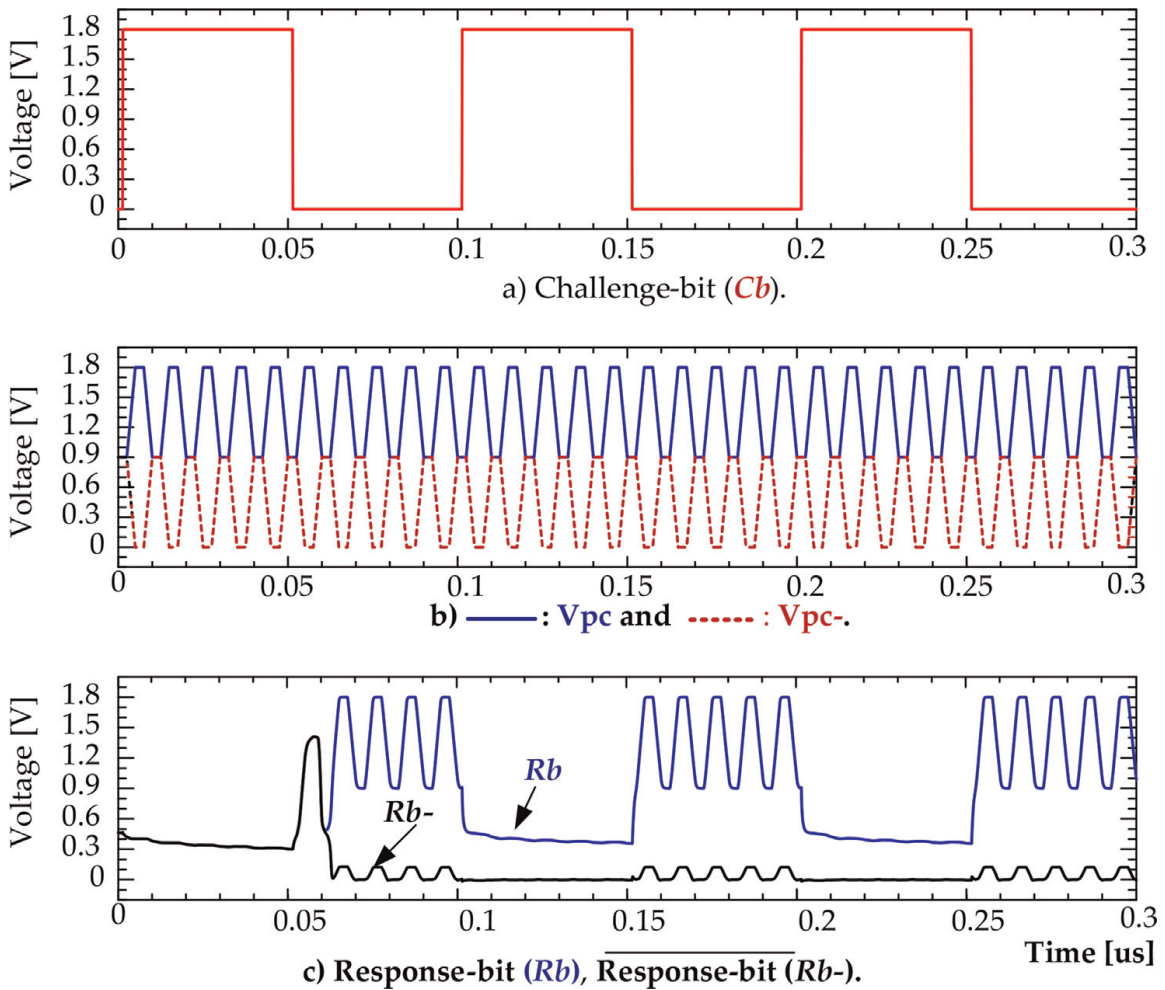


Figure 13. Input and output signals of the proposed CMOS TCPA-PUF cell with nominal 1.8 V of V_{dd} voltage.

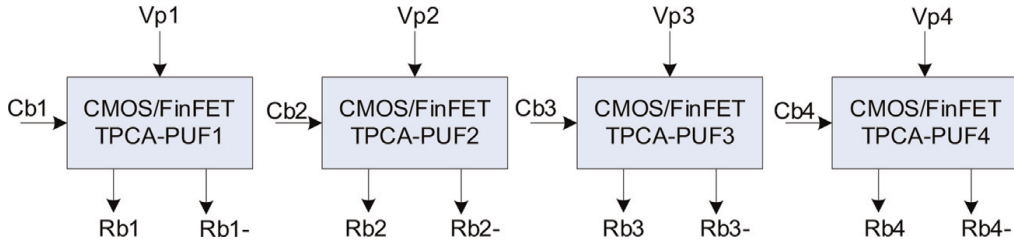


Figure 14.
Proposed 4-bit CMOS/FinFET TPCA-PUF architecture.

Moreover, each challenge bit signal has $\frac{1}{4}$ delay time of one power clock cycle. This delay time allows the challenge bits to flip the response signals right at the middle point of the idle/wait phase of the V_{pc} signals, and the challenge bits are perfectly flipped adiabatically.

Monte-Carlo simulation results of the 4-bit TPCA-PUF and QUAL-PUF challenge-response signals are depicted in **Figure 16**, where 100 times repetitions of the same 4-bit LSI PUF circuit are simulated. This result is performed with reference temperature of $T = 27^\circ\text{C}$ and $C_L = 10 \text{ fF}$, $f_{Cb} = 10 \text{ MHz}$, and $f_{Vpc} = 100 \text{ MHz}$ with $\pm 10\%$ of V_{th} variation. Simulation results of response signals (Rb1–Rb4) with a given challenge bit (Rb) performed correct and stable operations for both PUF circuit topologies.

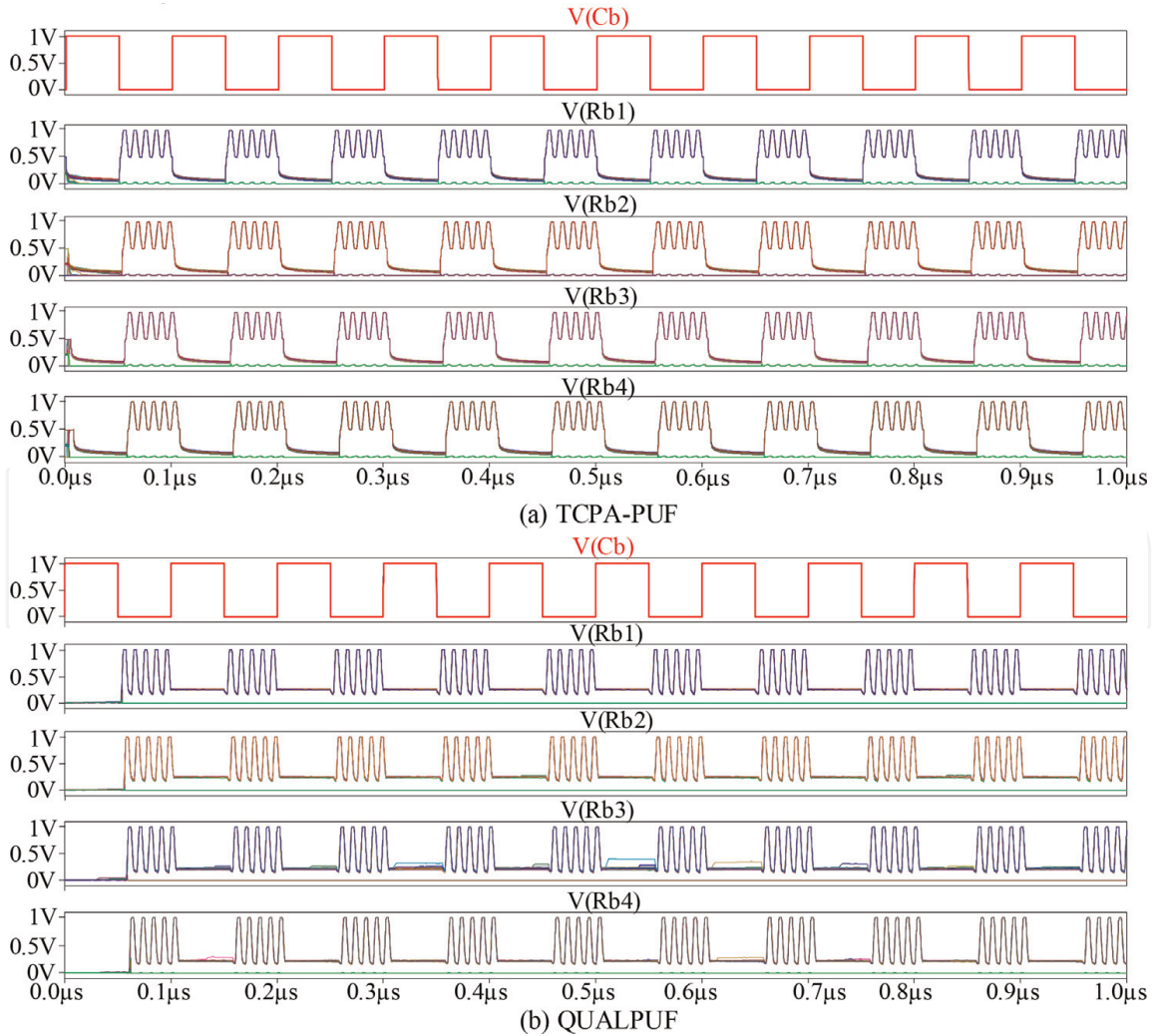


Figure 15.
Monte-Carlo simulation result of proposed 4-bit FinFET based TPCA-PUF LSI circuit with nominal 1 V of V_{dd} voltage.

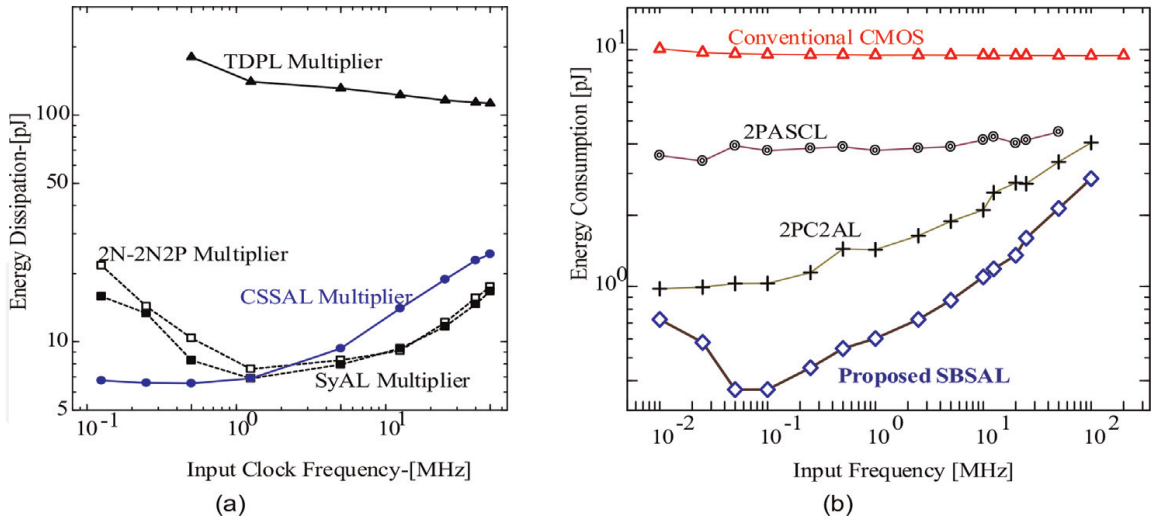


Figure 16. Energy dissipation of the LSI multiplier circuits; (a) bit parallel cellular multiplier over GF (2⁴) with secure CSSAL circuit (refer to **Figure 6**), (b) 4x4-bit array multiplier (refer to **Figure 10** with SBSAL circuit).

5. Simulation results and discussion

The simulation results presented in this section are all obtained from LTSpice simulation of both CMOS and FinFETs technologies, while the simulation conditions are described in **Table 1**.

The technical discussion in this paper will only focus on energy dissipation, which reflects the title of low-power of this paper. Energy dissipated by each LSI circuits is obtained from the following Eq. (17) formula:

$$E_{SBSAL} = \int_0^T (V_{pc(t)} I_{pc(t)} + V_{bias} I_{bias(t)}) dt, \quad (17)$$

and energy dissipation for both CSSAL and TCPA-PUF are formulated in Eq. (18):

$$E_{diss.} = \int_0^T \Sigma (V_{pcs} I_{pcs}) dt. \quad (18)$$

CSSAL and SBASL TCPA-PUF circuits	<ul style="list-style-type: none"> • V_{pc} Max.: 1.8 V with f_{V_{pc}}: 125 KHz–50 MHz (CSSAL Multiplier GF (2⁴) LSI) • V_{pc} Max.: 1.8 V with f_{V_{pc}}: 10 KHz–100 MHz (SBSAL 4x4-bit Multiplier LSI) • V_{pc}: swing from 0.9–1.8 V for CMOS trapezoidal clock (FinFETs: 0.5–1 V), f_{V_{pc}} = 100 MHz • V_{pc} -: swing from 0–0.9 V for CMOS trapezoidal power clock (FinFETs: 0–0.5 V), f_{V_{pc}} = 100 MHz • C_b voltage: 1.8 V CMOS pulse signal (FinFETs: 1 V), f_{C_b} = 10 MHz
Transistor parameter and ratio	<ul style="list-style-type: none"> • CMOS Parameter: 0.18 μm ROHM standard CMOS process with ratio W/L= 0.6 μm/ 0.18 μm for all NMOS and PMOS Transistors • FinFET Parameter: 45 nm with bulk, the ratio W/L = 60 nm/45 nm for all PMOS and NMOS Transistor

Table 1. Simulation conditions.

1. In CSSAL design process, the author has employed several techniques, such as (1) adopting the adiabatic switching principle for energy recycling to achieve low power consumption and low peak current, (2) dual-rail logic circuit topology is utilized to establish uniform transitional supply peak current, and (3) symmetric pull-down network transistors with internal node charges are shared and discharged to ground simultaneously, which construct a constant internal equivalent RC model for all input condition to reduce current-to-data dependency. The evaluation metric in our proposed CSSAL circuit has two targets: the secure logic and low power. For secure logic verification, we evaluate the logic ability to balance current traces by calculating the normalized standard deviation as in following Eq. (19):

$$\text{NSD} = \sigma_E / \bar{E}, \quad (19)$$

where the \bar{E} is the average of energy dissipation of every respective input transition, and the standard deviation of $\sigma_E = \sqrt{\sum_{i=E1}^{En} (E_i - \bar{E})^2 / n}$. The ideal value of NSD has to be 0%. The post-layout comparison of secure logic circuits in this paper is as labeled in **Figure 16a**, such as TDPL, SyAL, CSSAL, and the 2N-2N2P. The NSD result calculated at 1.25 MHz has shown that the CSSAL has 3.49%, SyAL: 4.69%, 2N-2N2P: 49.08%, and TDPL has 58.71%. Moreover, the energy dissipation per cycle of post-layout simulation is shown in **Figure 16a**, in which the proposed CSSAL consumes low energy at lower frequencies (1.25 MHz and below). Therefore, the proposed CSSAL cellular multiplier is suitable for low-power and high-security devices at 1.25 MHz and/or below this speed.

2. The energy of SBSAL is checked and compared with other adiabatic static logic families including conventional static CMOS logic as depicted in **Figure 16b**. It is obviously shown in this figure, the proposed SBSAL multiplier has reduced energy about 94% from conventional CMOS circuit, 84% from the 2PASCL circuit, and 58% from the 2PCAL circuit at 1~MHz operating frequency, and always consumes lower energy along the frequency band investigated in this work.
3. The proposed TCPA-PUF circuit stability has been verified in the 180 nm CMOS process and in 45 nm bulked FinFETS technology, where the proposed circuit has performed its superiority in terms of evaluation metrics (*Uniqueness* and *Reliability*) and low-power consumption than that of the QUAL-PUF one. The *Uniqueness* is used to determine the ability of a PUF to uniquely distinguish a chip among the other chips [28], as formulated in the following Eq. (20):

$$\text{Uniqueness } (U(\%)) = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^k \frac{HD(R_i, R_j)}{n} \times 100. \quad (20)$$

The *Reliability* measures how reproducibly the challenge-response pairs of a PUF instance with the varying environmental conditions such as temperature and CMOS process variations as shown in Eq. (21):

$$\text{Reliability } (R(\%)) = 100 - \frac{1}{k} \sum_{i=1}^k \frac{HD(R_i, R_{i,j})}{n} \quad (21)$$

PUF	QUAL-PUF [28]			Proposed TCPA-PUF	
	CMOS		FinFET	CMOS	FinFET
Year	2020		2021	2021 [29]	2021 [30]
Tech.	180 nm	45 nm	45 nm	180 nm	45 nm
Topology	Adiabatic SRAM			Adiabatic SRAM	
Transistor-number/bit	5	5	5	7	7
Process (nm)	180	45	45	180	45
Start-Up power	3.08 μ W	NA	65.69 nW	0.47 μ W	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

Table 2.

Comparison of conventional and proposed adiabatic PUFs (with $T = 27^{\circ}\text{C}$ and $C_L = 10 \text{ fF}$, $f_{\text{Cb}} = 10 \text{ MHz}$, and $f_{\text{Vpc}} = 100 \text{ MHz}$).

The ideal values of *uniqueness* and *reliability* are 50% and 100%, respectively. The TCPA-PUF evaluation results have always been close to the ideal values.

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 [44], and its double gates enabling three possible connection modes (shorted gate-SG, independent gate-IG, and low-power-LP) for low power and high-speed applications. In this work, the author has thoroughly investigated the proposed TPCA-PUF cell using bulked FinFET with a 45 nm process for all SG, IG, and LP modes. As a result, the author has revealed that SG mode is suitable for the proposed TPCA-PUF circuit topology. The gate connection type of LP and IG modes leads to higher energy and produces wrong response bits for larger cascaded bit-length (4-bit in this work). Therefore, the whole works of 4-bit LSI design and simulation, including the data presented in this paper are performed by utilizing the SG mode connection type. The TPCA-PUF cell was implemented using SRAM-based circuit topology, hence this study is claimed to be the first work in the literature that employs FinFETs-based SRAM type PUF. Numerical data in **Table 2** compare the QUAL-PUF and proposed TPCA-PUF for both CMOS and FinFETs process technologies. Overall data in **Table 2** have shown that the proposed TPCA-PUF consumes lower energy/bit/cycle and start-up power, which is suitable for low-power IoT application.

6. Conclusion

This paper has presented a comparative study on energy dissipation and secure evaluation metrics of the proposed CSSAL, SBSAL, and QUAL-PUF with other conventional related circuit topologies.

1. Secure CSSAL: the NSD result calculated at 1.25 MHz has shown that the CSSAL has 3.49%, SyAL: 4.69%, 2N-2N2P: 49.08%, and TDPL has 58.71%. Moreover, the energy dissipation per cycle of post-layout simulation has shown that the

CSSAL consumes low energy at lower frequencies (1.25 MHz and below). Therefore, the proposed CSSAL cellular multiplier is suitable for low-power and high-security devices at 1.25 MHz and/or below this speed.

2. Low-Power SBSAL: Simulation results have shown that the proposed SBSAL multiplier has reduced energy about 94% from conventional CMOS circuit, 84% from the 2PASCL circuit, and 58% from the 2PCAL circuit at 1~MHz operating frequency.
3. TPCA-PUF: the SRAM-based CMOS and FinFETs PUF using 180nm and 45 nm technology process, respectively, has been further investigated into 4-bit cascaded bitlength, where the proposed TPCA-PUF has reduced energy/bit/cycle and start-up power, both about 70% from the QUAL-PUF cell at the same reference temperature of 27°C.

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


Author details

Cancio Monteiro

Faculty of Engineering Science and Technology, Department of Electronics and Electrical Engineering, National University of Timor Lorosa'e (UNTL), Dili, Timor-Leste

*Address all correspondence to: cancio.monteiro@untl.edu.tl

IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Bojan J. Internet of Things statistics for 2022 – Taking Things Apart. DataProt. 2022. Available online: <https://dataprot.net/statistics/iot-statistics/> (update: May 13, 2022; Accessed: July 2, 2022)
- [2] Atzori L, Iera A, Morabito G. The internet of things: A survey. *Computer Networks*. 2010;**54**:2787-2805
- [3] Bandyopadhyay D, Sen J. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*. 2011;**58**:49-69
- [4] Keoh SL, Kumar SS, Tschofenig H. Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal*. 2014;**1**: 265-275
- [5] Sicari S, Rizzardi A, Grieco L, Coen-Porisini A. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*. 2015;**76**:146-164
- [6] 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; 2010
- [7] Wurm J, Hoang K, Arias O, Sadeghi AH, 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; 2016. pp. 519-524
- [8] 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; 2017. pp. 312-321
- [9] Martinez B, Montón M, Vilajosana I, Prades JD. The power of models: Modeling power consumption for iot devices. *IEEE Sensors Journal*. 2015;**15**: 5777-5789
- [10] Mukhopadhyay SC, Suryadevara NK. Internet of things: Challenges and opportunities. In: *Internet of Things*. Berlin/Heidelberg, Germany: Springer; 2014. pp. 1-17
- [11] 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; 2014. pp. 697-701
- [12] Paul K. Timing attacks on implementation of Diffie-Hellman, RSA, DSS and other system. In: *Proceedings of the 16th Annual International Cryptology Conference*, Santa Barbara, California, USA. 1996. pp. 104-113
- [13] Erick O, Rincón-Mora GA. Electrostatic energy-harvesting and battery-charging CMOS system prototype. *IEEE Transactions on Circuits and Systems*. 2009;**56**:1938-1948
- [14] Kocher P, Jaffe J, Jun B. Differential power analysis. *Proceedings of the International Advances in Cryptology Conference (CRYPTO)*. 1999:388-397
- [15] Elke DM, Siddika BO, Bart P, Ingrid V. Differential electromagnetic attack on an FPGA implementation of elliptic

- curve cryptosystems. In: Proceedings of World Automation Congress (WAC'06), Budapest, Hungary. 2006. pp. 1-6
- [16] Eric B, Christophe C, Francis O. Correlation power analysis with a leakage model. In: Proc. Sixth Int. Workshop on CHES 2004, Cambridge, MA, USA: LNCS; 2004. pp. 16-29. DOI: 10.1007/978-3-540-28632-5-2
- [17] Athas WC, Svesson LJ, Koller JG, Trautzanis N, Chuo EY-C. Low power digital system based on adiabatic-switching principles. *IEEE Transactions on Very Large Scale Integration System.* 1994;2:398-406
- [18] Khatir M, Moradi A. Secure adiabatic logic: A low energy DPA resistant logic style. *Cryptology ePrint Archive*, 2008. <https://ia.cr/2008/123>
- [19] Choi BD, Kim KE, Chung K-S, Kim D. Symmetric adiabatic logic circuits against differential power analysis. *ETRI Journal.* 2010;32(1):166-168
- [20] Kramer A, Denker JS, Flower B, Moroney J. 2nd Order Adiabatic Computation 2N-2P and 2N-2N2P Logic Circuits. In: Proceedings of IEEE International Symposium on Low Power Design, Dana Point California, USA. 1995. pp. 191-196
- [21] Moradi A, Khatir M, Salmasizadeh V, Shalmani MTM. Investigating the DPA-resistance property of charge recovery logics. *IACR ePrint Archive.* 2008, pp. 191—192
- [22] Cancio M, Yasuhiro T, Toshikazu S. Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attack at cell level. *Microelectronics Journal.* 2013;44:496-503
- [23] Amit D, Himanshu T. 2-Phase adiabatic logic for low-energy and CPA-resistant implantable medical devices. *IEEE Transactions on Consumer Electronics.* 2022;68(1):47-56
- [24] Moshe A, Hadar D, Itamar L, Osnat K, Alexander F. DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing s-boxes. *IEEE Transactions on Circuits and Systems.* 2015;62(1): 149-156
- [25] Charles H, Meng-day Y, Farinaz K, Srinivas D. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE.* 2014;102(8): 1126-1141
- [26] Debdeep M. PUFs as promising tools for security in Internet of Things. *IEEE Design & Test.* 2016;33(3):103-115
- [27] Thomas MG, Ibrahim EB, Zhiming MW, Utz R, Robert JY. A PUF taxonomy. *Applied Physics Reviews.* 2019;6:011303
- [28] Kumar SD, Thapliyal H. Design of adiabatic logic-based energy-efficient and reliable PUF for IoT devices. *Journal of Emerging Technologies in Computing System.* 2020;16:34
- [29] Cancio M, Yasuhiro T. Low-power two-phase clocking adiabatic PUF circuit. *Electronics.* 2021;10:1258
- [30] Cancio M, Yasuhiro T. Ultra-low power FinFETs-based TPCA-PUF circuit for secure IoT devices. *Sensors.* 2021; 21(4):8302
- [31] Veendrick HJM. Short-circuit dissipation of static CMOS circuitry and its impact on the design of buffer circuits. *IEEE Journal of Solid-State Circuits.* 1984;19(4):468
- [32] De V, Ye Y, Keshavarzi A, Narendra S, Kao J, Somasekhar D, et al.

- Techniques for leakage power reduction. In: Book of Design of High-Performance Microprocessor Circuits. Wiley-IEEE Press; 2001
- [33] Lu Y, Agraval VD. CMOS leakage and glitch minimization for power performance tradeoff. *Journal of Low Power Electronics*. 2006;2(3):378
- [34] Panda PR, Shrivastava A, Silpa BVN, Gummidipudi K. *Power Efficient System Design*. New York: Springer; 2010
- [35] Tran DJ, Acuff MJ. Dynamic logic circuit. United States Patent:5,859,547. 1999
- [36] Moon Y, Jeong DK. An efficient charge recovery logic circuit. *IEEE Journal of Solid-State Circuits*. 1996; 31(4):514-522
- [37] Yasuhiro T, Toshikazu S, Yokoyama M. VLSI implementation of a 4x4-bit multiplier in a two-phase drive adiabatic dynamic CMOS logic. *IEICE Transactions on Electronics*. 2007;E90-C(10):2002-2006
- [38] Yasuhiro T, Toshikazu S, Yokoyama M. Two-phase clocked CMOS adiabatic logic. *Journal of Electronics and Communications*. 2009; 3(1):17-34
- [39] Nazrul AN, Yasuhiro T, Toshikazu S. LSI implementation of a low-power 4×4-bit array two-phase clocked adiabatic static CMOS logic multiplier. *Microelectronics Journal*. 2012;43(4): 244-249
- [40] Kazunari K, Yasuhiro T, Toshikazu S. Two phase clocked subthreshold adiabatic logic. *IEICE Electronic Express*. 2015;12(20):1-12
- [41] Cancio M, Apolinario M, Yasuhiro T. Low power source biased semi-adiabatic logic circuit for IoT devices. In: *Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS'18)*. Okinawa-Japan; 2018. pp. 43-47
- [42] Tiri K, Akmal M, Verbauwhede I. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In: *Proceedings of European Conf. Solid-State Circuits (ESSCIRC '02)*. Firenze, Italy; 2002. pp. 403-406
- [43] Bucci M, Giancane L, Luzzi R, Trifiletti V. Three-phase dual-rail pre-charge logic. In: *Proceedings of CHES'06*, Yokohama Japan; 2006. pp. 232-241
- [44] King TJ. FinFETs for nanoscale CMOS digital integrated circuits. In: *Proceedings of IEEE/ACM International Conference on Computer-Aided Design*. San Jose; 2005. pp. 207-210