IET Information Security

Research Article

IET Journals
The Institution of Engineering and Technology

Charge balancing symmetric pre-resolve adiabatic logic against power analysis attacks

ISSN 1751-8709
Received on 16th April 2018
Revised 18th July 2019
Accepted on 15th August 2019
E-First on 26th September 2019
doi: 10.1049/iet-ifs.2018.5136
www.ietdl.org

Prathiba Ashok[1], Kanchana Bhaaskaran Vettuvanam Somasundaram[1] ✉

[1]*School of Electronics Engineering, VIT University, Chennai, India*

✉ *E-mail: vskanchana@ieee.org*

Abstract: A novel, energy efficient and power analysis robust logic style called the charge balancing symmetric pre-resolve adiabatic logic (CBSPAL) is proposed to overcome the susceptibility of cryptosystems against side channel power analysis attacks. It employs differential cascode logic tree structure with a pre-resolving feature, which realises improved energy efficiency by minimising non-adiabatic loss and leakage current. The energy efficiency of the proposed logic against static complementary metal oxide semiconductor (CMOS) and other existing secure adiabatic logic styles is proved. Energy deviation for the different input transitions of the individual logic gates, namely, buffer/NOT, AND/NAND and XOR/XNOR is found to be very minimal and it validates the immunity of the proposed logic against power analysis attacks. SPICE simulation of 4-bit add-round structure implementation using CBSPAL shows an energy saving of 89.5% compared to static CMOS implementation at a frequency of 125 MHz. Security of the proposed logic against the side channel power analysis attack is demonstrated by performing the correlation power analysis attacks as applicable for the SPICE simulations. Exhaustive SPICE simulations have been performed using the 32 nm CMOS predictive technology model libraries.

1 Introduction

The cyber physical systems (CPS) and internet of things (IOT) establish smart connectivity across the systems. They demand effective security solutions. These systems are constrained in terms of power and area and their security is mandated to be addressed by lightweight cryptography [1]. Lightweight cryptography offers an adequate level of security using lightweight, compact and low power algorithms/operations. CPS and IOT systems are pervasive in nature. They are physically accessible which makes them susceptible to side channel attacks. Side channel attacks are the attacks over physical implementation which concentrates on timing, power and electromagnetic interference to identify the secret information. Power analysis attacks are non-invasive and they pose a dominant threat in comparison with other side channel attacks. Counteracting power analysis attacks is a primary concern in the design of security hardware. Power analysis counter measures have been addressed in various levels of abstractions, namely, system level, algorithmic level, and circuit level. Lower the level of abstraction better is the security offered by the counter mechanism. The circuit level counter measures offer promising security solutions.

Among the circuit level techniques, secure adiabatic logics have been proven the effective solutions for the design of power analysis attack resistant circuits, with low power consumption and high energy efficiency [2–9]. Adiabatic logic inherits the principle of charge recovery to achieve energy efficiency [10, 11]. The mechanisms employed in the existing secure adiabatic logic designs employ various strategies to improve energy efficiency and many counter measures to thwart power analysis attacks [12]. The mechanisms widely presented are summarised as follows:

- Symmetric discharge paths and charge sharing between differential or complementary nodes protect the circuit against power analysis attacks in the symmetric adiabatic logic families [10]. Side-channel information leakage is prevented by reduction of data-dependent energy dissipation in secured-quasi-adiabatic logic (SQAL) and Symmetric adiabatic logic (SYAL) logic styles [4].
- In the symmetric pass gate adiabatic logic (SPGAL), the energy efficiency is improved by the reduction of non-adiabatic energy loss. Security of the SPGAL family is realised by reset of output before every evaluation [5].
- Leakage current is a dominant factor due to technology scaling, the use of emerging alternative devices namely, fin field effect transistor and tunnel field effect transistor structures have been addressed in the literature for reduced leakage and low power. The adiabatic or energy recovery method is also employed to improve energy efficiency [8, 13].

The other circuit level approaches widely analysed for design of security hardware are the complementary metal oxide semiconductor (CMOS)-based dynamic logic structure with two-phase and three-phase operations [14–18]. Even though these types of logic styles were able to provide promising security solutions, their power capabilities are not found attractive enough and they are not found suited to lightweight and low power applications.

The main objective in this work is the design of a novel, energy efficient, low power and power analysis robust adiabatic logic style suited to lightweight smart devices. The individual logic gates using the proposed charge balancing symmetric pre-resolve adiabatic logic (CBSPAL) exhibit lower energy consumption across the range of frequencies as compared against the existing differential power analysis (DPA) resistant adiabatic logic family in the literature. The overall energy efficiency of the proposed logic is improved by elimination of leakage path. Charge balanced circuit construction, data dependence elimination, low peak current, and low energy deviation are the reasons for the resistance of the proposed logic against power attacks. The resistance of the proposed style against the correlation power analysis (CPA) attacks is verified by using the correlation-based analysis on 4-bit add-round architecture implementation.

Section 2 explains the pre-resolve energy efficient logic design and its functional operation. Section 3 presents the energy metrics of CMOS logic and CBSPAL adiabatic logic. Section 4 analyses the power attack resistance of the proposed logic and Section 5 presents the implementation of an add-round test circuit and the correlation-based security analysis. Section 6 concludes the paper.

2 CBSPAL structure and functional operation

The CBSPAL logic enhances the efficiency of differential cascode pre-resolve adiabatic logic (DCPAL)-based circuit for secure adiabatic logic style by employing additional charge balancing transistors, which balances the potential across *out* and *out_bar* nodes. DCPAL focuses on design of low power circuit design for arithmetic circuits [19]. The proposed logic aims at improving energy efficiency over the existing DPA resistant adiabatic logic families by pre-resolving the inputs to zero before evaluation [20]. The adiabatic circuits by their inherent architecture always draw constant current from its power clock, which is used to charge the output node or the complementary node. This is due to the differential or sense amplifier structured latch in the pull up network. Therefore, irrespective of the state of output node (or its complementary node), the current spent by the power clock remains the same. This, in other words, amounts to the fact that the adiabatic load presented to the power clock always remains the same, irrespective of the data being processed by the charge recovery logic. This factor has been exploited for design of DPA resistant circuits. Fig. 1 shows the schematic diagram of the proposed pre-resolve-based CBSPAL buffer. A four-phase trapezoidal clock used for powering the circuit is shown in Fig. 2. Two cross-coupled p-type metal oxide semiconductor (pMOS) transistors M1 and M2 together act as latch to provide output charging/discharging paths for evaluation and recovery. The logic structure for the functional evaluation is obtained by replacing the pull down n-type metal oxide semiconductor (nMOS) transistors M4 and M5 as per relevant logic function required. The power clock PC3 is ahead of the power clock PC1 by 180°. The pre-resolving is enabled by applying the pulse PC3 at the gate terminal of M3. Discharge pulse is a trapezoidal pulse with timing relationships set as shown for power clocks PC1 and PC3 in Fig. 3. The discharge pulse is two times the power clock frequency. The benefits offered by the DCPAL [19] structure to improve energy efficiency is

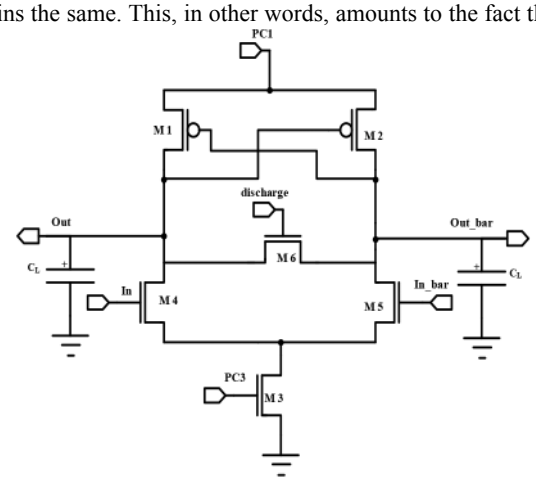

Fig. 1 *CBSPAL buffer*

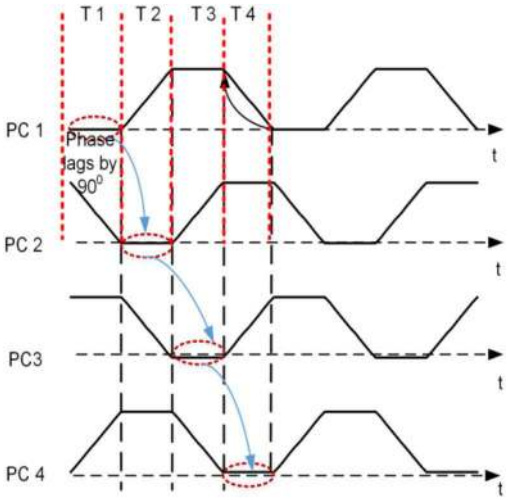

Fig. 2 *Four-phase clocking mechanism*

- Pre-resolving the output nodes before evaluation.
- Isolating the supply power from the evaluation block during the pre-resolve phase to eliminate the short circuit path between the ground and the supply.
- Isolating the ground from the evaluation block during the recovery phase to avoid the leakage path formation between the supply and the ground.

The proposed pre-resolve buffer operates in four phases: (i) pre-resolve based on input to zero, (ii) evaluate, (iii) hold, and (iv) recover. Let us assume that all nodes are at ground initially. The functional operation of the buffer during various operating phases is explained as follows.

T1 (pre-resolve phase): during T1, consider *In* rises and *In_bar* is low, and PC3 is at its peak amplitude. Then, M3 conducts and connects the source of M4 and M5 to the ground. As *In* reaches the threshold v_{tn} of the nMOS device M4, it conducts to make the inputs pre-resolved and *Out* becomes low. Switching operation of the transistors during the T1 phase is shown in Fig. 4. In this phase, the discharge pulse slowly rises to discharge any charge stored in the nodes during the previous cycle.

T2 (evaluate phase): during T2, PC3 falls, and as the gate voltage of M3 falls below v_{tn}, it ceases to conduct and the output remains low by the charge stored in the *Out* load capacitance. Simultaneously, PC1 rises and M2 turns on with *Out_bar* slowly rising with PC1 as shown in Fig. 5. During this phase, the discharge signal and the input signal *in_bar* are at ground. The transistor M5 is off and the leakage current due to the stacking of nMOS transistors M5 and M3 is negligible.

T3 (hold phase): during T3, *in* goes low and *Out* and *Out_bar* retains their value with the help of the pMOS latch formed by M1 and M2. PC3 is low and M3 is completely off. The operation of this phase is shown in Fig. 6.

T4 (recovery phase): during T4, PC1 goes low, and the charge recovery path is established between the *Out_bar* and PC1, the charge recovers through the path M2 as shown in Fig. 7. The

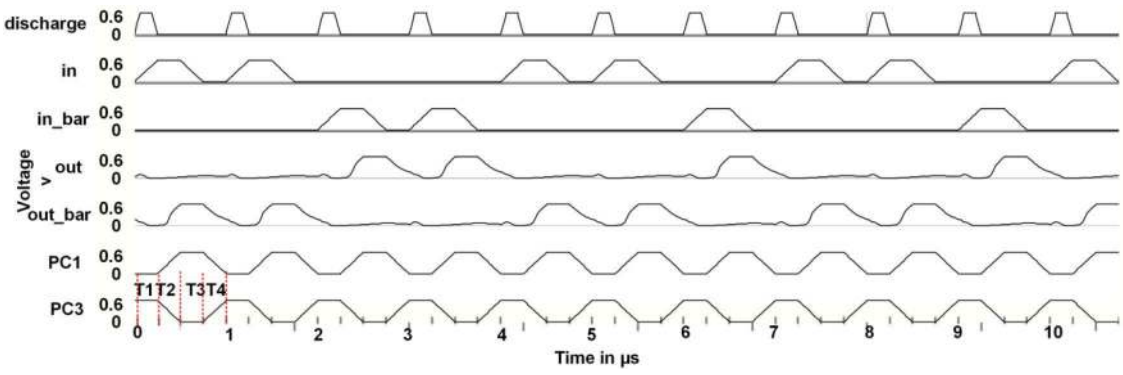

Fig. 3 *Timing diagram of the power clocks and the input–output signals*

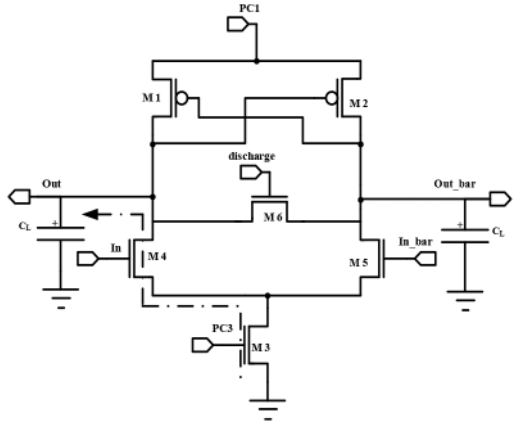

Fig. 4 *Pre-resolve phase*

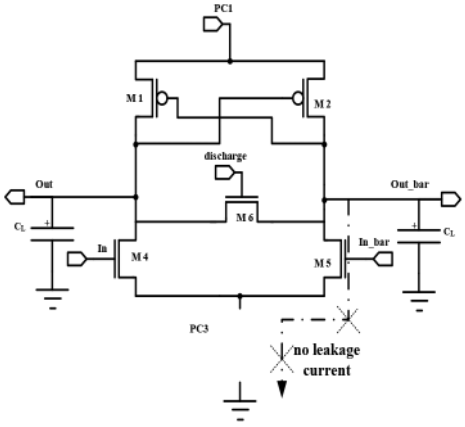

Fig. 6 *Output hold phase*

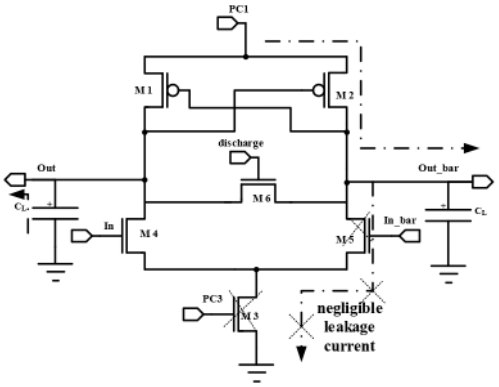

Fig. 5 *Rising output with the supply power clock*

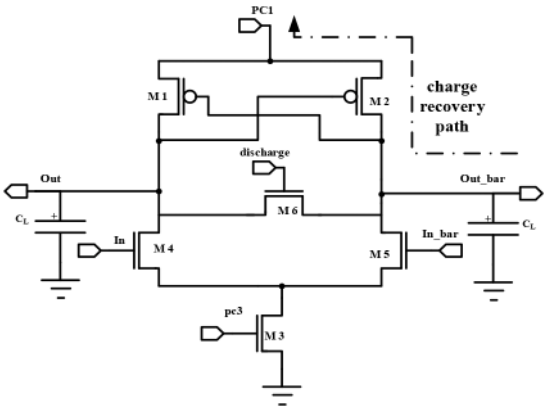

Fig. 7 *Charge recovery phase*

charge stored in the output node at the end of every T (T1–T4) before the beginning of the next clock cycle is discharged by the discharge signal. Since the charge stored is discharged before every evaluation, the correlation between the input signal and the supply current is eliminated.

3 Static CMOS and CBSPAL adiabatic logic – comparison of energy metrics

In a static CMOS circuit, the total energy consumption is given by [19]

$$E_{\mathrm{CMOS}} = E_{\mathrm{switching}} + E_{\mathrm{sc}} + E_{\mathrm{leak}}$$

where E_{sc} and E_{leak} are energy losses due to short circuit current and leakage current. The total energy incurred for the switching event of a static CMOS circuit is $C_{\mathrm{L}}V_{\mathrm{DD}}^2$, where V_{DD} is the supply voltage. The energy consumption per switching event of a quasi-adiabatic circuit is given by [19–22]

$$E_{\mathrm{quasi\text{-}adia}} = E_{\mathrm{adia}} + E_{\mathrm{non\text{-}adia}} + E_{\mathrm{leak}} + E_{\mathrm{latch}}$$

where E_{adia} is the adiabatic energy dissipated in the switching device for a linear ramp input. The adiabatic loss is dependent on the frequency of operation, the charging path resistance, the supply voltage, the sizing of devices, and the total physical capacitive loading. $E_{\mathrm{non\text{-}adia}}$ is the non-adiabatic energy loss, E_{leak} is the loss in energy due to the subthreshold leakage of the non-conducting transistors and E_{latch} is the energy dissipation in the pMOS-based latch.

The proposed CBSPAL reduces the non-adiabatic energy dissipation due to its differential cascode voltage switch tree structure. The leakage loss is eliminated in CBSPAL by its unique power clocking mechanism. This section discusses the individual energy components incurred by the CBSPAL in the different phases of operation. As the output node is pre-resolved to zero, there exists no potential difference between the source and drain node of the footer transistor M3 shown in Fig. 8*a*. The absence of potential difference between ground (source) and output (drain) node eliminates the non-adiabatic energy loss at the output node during the pre-resolve phase. However, there is non-adiabatic energy dissipation during pre-resolving, proportional to the gate capacitance of the pre-resolving transistor given by E_{loss1}. Another non-adiabatic energy loss factor, E_{loss2} is due to the gate capacitance of the discharge transistor. The pre-resolve transistor M3 and the discharge transistor M6 are *on* during the pre-resolve phase and both E_{loss1} and E_{loss2} occur during every pre-resolve phase and they are independent of frequency. During the evaluate phase, the pMOS transistor M2 will be *on* when the voltage level reaches its threshold level V_{tp}. This leads to adiabatic charging of output node *out_bar* as shown in Fig. 8*b*. The adiabatic energy loss for the linear ramp input when $T \gg R_{\mathrm{p}}C_{\mathrm{L}}$ is given by [19]

$$E_{\mathrm{adia}} = \left(\frac{R_{\mathrm{p}}C_{\mathrm{L}}}{T}\right)C_{\mathrm{L}}V_{\mathrm{dd}}^2$$

where R_{p} is the effective resistance of the pMOS in the charging path, V_{dd} is the peak voltage of supply power clock, T is the transition period of power clock and C_{L} is the output nodal capacitance. This phase also exhibits a non-adiabatic loss E_{loss4} expressed as $(1/2)CV_{\mathrm{tp}}^2$ proportional, where V_{tp} is the threshold voltage of the pMOS device. This energy loss is exhibited only when the output switches from logic 1 to 0 between the successive cycles in any one of the complementary output nodes. During the hold phase, both M4 and M5 are off as shown in Fig. 8*c*. Also, the energy consumed is due to the pMOS latch operation viz., E_{latch}. In the charge recovery phase, the power clock ramps down to zero and the charge from the *out_bar* node, which is indicated in adiabatic state T2 (evaluate phase) is recovered through the path shown in Fig. 8*d*. Hence, the total energy loss of the proposed CBSPAL can be represented by

$$E_{loss} = E_{loss1} + E_{loss2} + E_{adia} + E_{loss4} + E_{latch} + E_{leak}$$

where the factor E_{leak} takes into account the leakage current flowing through the non-conducting transistors. The *on* transistor is represented by a resistor in the RC model.

4 Analysis of power attack resistance of the proposed logic

The proposed logic exhibits the desirable characteristics for the logic circuit to possess power analysis robustness. The features necessary to exhibit power attack resistance in the circuit level are

- charge balanced and symmetric circuit structure
- data dependency elimination
- low peak current and low energy deviation

To evaluate the performance of the proposed logic style, the individual logic gates buffer/NOT, AND/NAND, XOR/XNOR and 4-bit add-round test circuit are simulated using SPICE tools with the 32 nm CMOS predictive technology model libraries [23]. The widths and lengths of the transistors are 96 and 32 nm, respectively, for both the pMOS and nMOS transistors with the load capacitance of 10 fF. The analysis is carried out for different frequencies, namely, 1.25, 12.5, and 125 MHZ. Results and analysis of each of the characteristics using the simulation are demonstrated for the CBSPAL logic in the following subsections and is compared against the existing secure adiabatic logic styles. Note that all the simulation results mentioned in the study are under the same simulation environment with the same technology node.

4.1 Charge balanced and symmetric circuit construction

The proposed pre-resolve-based logic employs charge balanced symmetric circuit construction as in SYAL and Charge-sharing symmetric adiabatic logic (CSSAL) [2, 10]. Table 1 presents the symmetric on–off pattern as realised in the pull down structures 1 and 2 designated as PDN-1 and PDN-2 for different input patterns. Transistors in the pull down path are arranged such that the on and off states are equal for all possible input patterns. Adoption of the charge balanced construction equalises the nodal voltages and eliminates any possible asymmetric behaviour for different input patterns. This feature also leads to balanced current consumption for every input transition. A charge balancing phenomenon for all possible input transitions is depicted using the RC model of the PDN during evaluation phase in Fig. 9. Charge balanced nature of the logic is evident as is proved for AND/NAND logic gate, for all possible input combinations as shown in Figs. 9*a*–*d*. Uniform supply current consumption for the logics, buffer/NOT and XOR/XNOR in different frequency ranges is exhibited as seen in Figs. 10*a* and *b*. These simulation results verify the charge balancing of the proposed logic.

4.2 Data dependency elimination

Hamming weight and Hamming distance are the most commonly used metrics to identify the transitional power fluctuation between different input transitions. Power consumption for the transition of input patterns from 0 to 0 and 1 to 1 is relatively less compared to the power variation incurred for the input transition from 0 to 1 or 1 to 0 while designing using static CMOS circuits. This feature ends up serving as the source of information leakage for systems implemented using static CMOS logic. The sense amplifier structured quasi-adiabatic logic circuit due to its inherent circuit topological advantage presents a constant load to power clock supply irrespective of any possible input transitions. However, the quasi-adiabatic charge by its very nature incur some charge losses remaining unrecovered and such nodes having unrecovered charge will make the system data dependent between successive evaluations. The supply current dependence on the input transitions is eliminated by the discharge of residual voltage before every evaluation. Discharge of the residual charge in the *out* and *out_bar* nodes for the buffer arrangement with $in = 1$ and $in\_bar = 1$ as depicted in Figs. 11*a* and *b*, respectively.

Elimination of data dependency between successive inputs is realised due to the application of the discharge pulse, which enables the compensation of the unrecovered charge between the output nodes out and *out_bar*. Hence, the information dependence between successive evaluations is removed. The output waveforms depicting the discharge of output (out or *out_bar*) node voltage to the ground due to the presence of discharge pulse is depicted from the simulation waveforms shown in Fig. 12. The internal node capacitances are also discharged to ground before the arrival of the next input signal by the discharge signal. As the discharge signal applied at the gate of transistor M6 of the CBSPAL buffer reaches its threshold V_{tn}, it becomes on and establishes a discharge path for charge stored during the previous cycle. This mechanism leads to the robustness of the proposed logic against power attacks. In other words, this arrangement makes the circuit style more suitable for security applications.

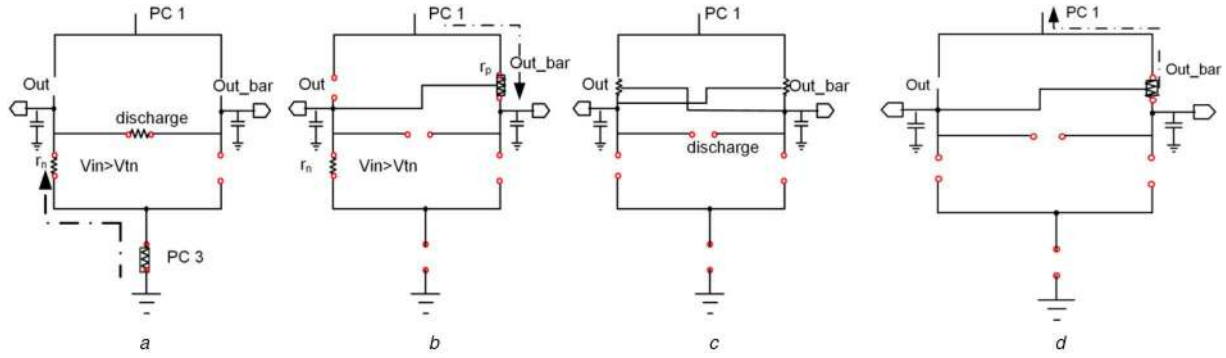

Fig. 8 *Timing phases of operation*
(a) Pre-resolving phase, ***(b)*** Evaluation phase, ***(c)*** Hold phase, ***(d)*** Charge recovery phase

Table 1 Charge balanced construction

	AND/NAND logic gate			
AB	00	01	10	11
PDN-1	*off–off*	*off–on*	*on–off*	*on–on*
	off–on	*on–on*	*off–off*	*on–off*
PDN-2	*on–off*	*on–off*	*off–on*	*off–on*
	on–on	*off–off*	*on–on*	*off–off*

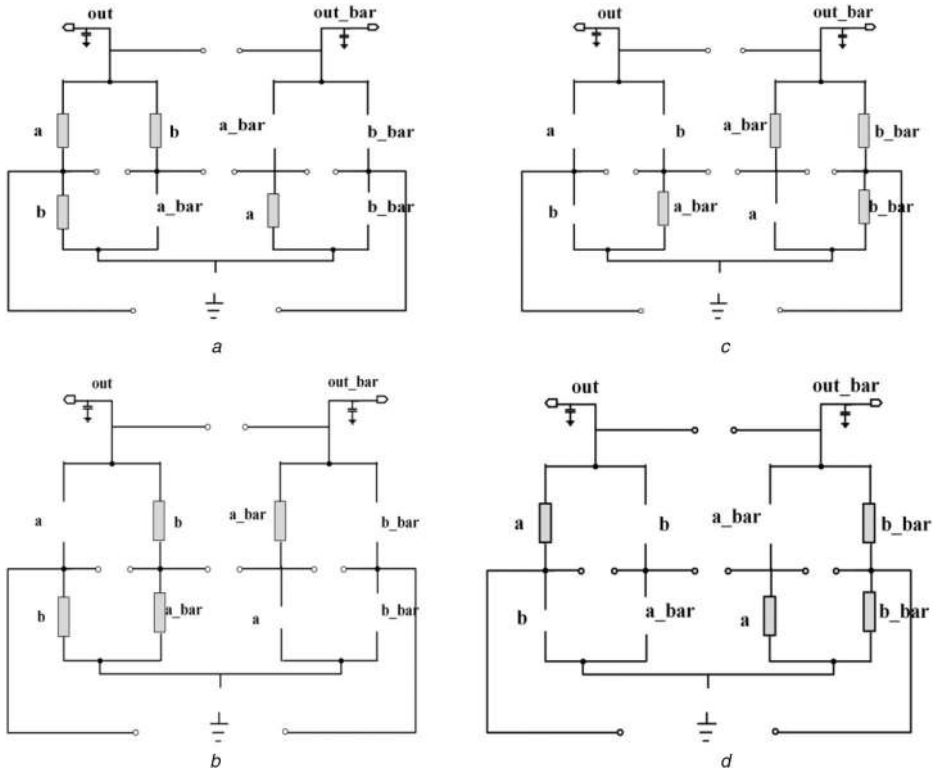

Fig. 9 *RC models of individual logics for different input combinations showing charge balanced structure*
(a) AND/NAND: AB-11, ***(b)*** AND/NAND: AB-01, ***(c)*** AND/NAND: AB-00, ***(d)*** AND/NAND: AB-10

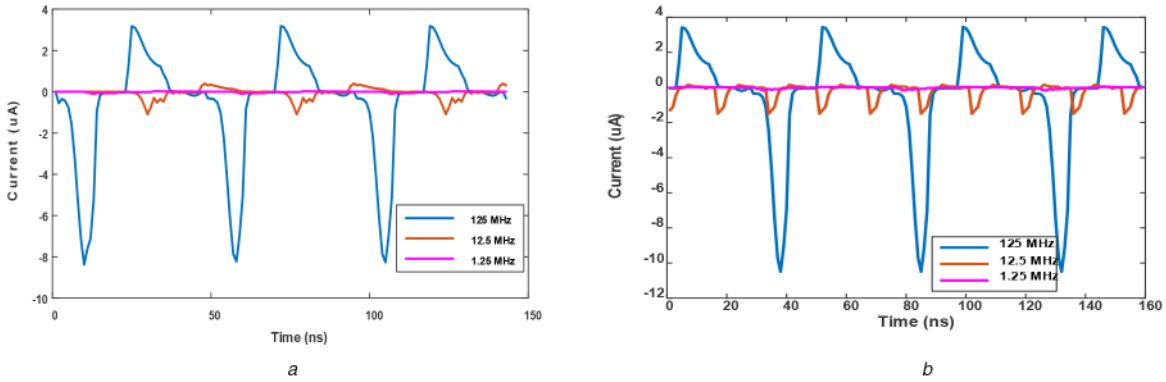

Fig. 10 *CBSPAL supply current waveforms of individual logics*
(a) Buffer/ NOT traces, ***(b)*** XOR/XNOR traces

4.3 Low-peak current and low-energy deviation

The realisation of a uniform pattern of current ensures the absence of transitional power variation. The low-energy deviation is an added feature, which contributes to the increased robustness against power attacks. Furthermore, the low-peak current value of the CBSPAL makes it more attractive for low-power applications.

The energy consumption of the proposed buffer is found to be low while operating at 1.25, 12.5 and 125 MHz, in comparison with the SYAL, SPGAL and energy-efficient (EE)-SPFAL buffers. The results are depicted in Table 2. Simulation results pertaining to the energy consumption per cycle of EE-SPFAL and CBSPAL individual logic gates are shown in Fig. 13 and the results validate the energy efficiency of CBSPAL buffer. Individual logic gates, namely, XOR and AND gates are found to realise an average energy reduction of 37% at 1.25 and 12.5 MHz in comparison with the EE-SPFAL. This is in line with the reasoning behind the improved energy efficiency of the DCPAL circuit against the 2 NMOS-2 PMOS, 2 NMOS 2NMOS 2PMOS, Improved pass-gate adiabatic logic and Positive feedback adiabatic logic counterparts [19].

Histogram of the energy consumption per cycle shown in Fig. 14 compares the energy deviation for different energy samples of CBSPAL XOR/XNOR against EE-SPFAL XOR/XNOR logic gates. Transitional energy fluctuations of smaller margins compared against the EE-SPFAL logic indicates the fact that the proposed logic incurs minimum energy deviation. Increased number of simulation observations of CBSPAL incurs less energy and distribution of energy is also found to be minimal relative to the EE-SPFAL with a similar input pattern under the same simulation environment. Furthermore, the energy values are concentrated to the lower end of spectrum. Lower energy consumption and reduced energy deviation are the two most desired features of a secure circuit style, to realise both energy efficiency and security against power attacks. The minimal energy deviation proves the resistance characteristics of the proposed logic against DPA attacks. Uniform instantaneous supply peak current of the CBSPAL style is evident from Fig. 15 depicting the individual XOR/XNOR and AND/NAND gates for various input patterns, viz. $AB = 00, 01, 10$ and 11. CBSPAL records lower peak current compared against its counterpart EE-SPFAL logic style.

Leakage current is a dominant factor in determining the energy efficiency and power attack resistance of secure circuit architectures. EE-SPFAL is a modified version of PFAL family, while the proposed CBSPAL circuit is built based on the DCPAL style as stated earlier. The number of leakage paths between the

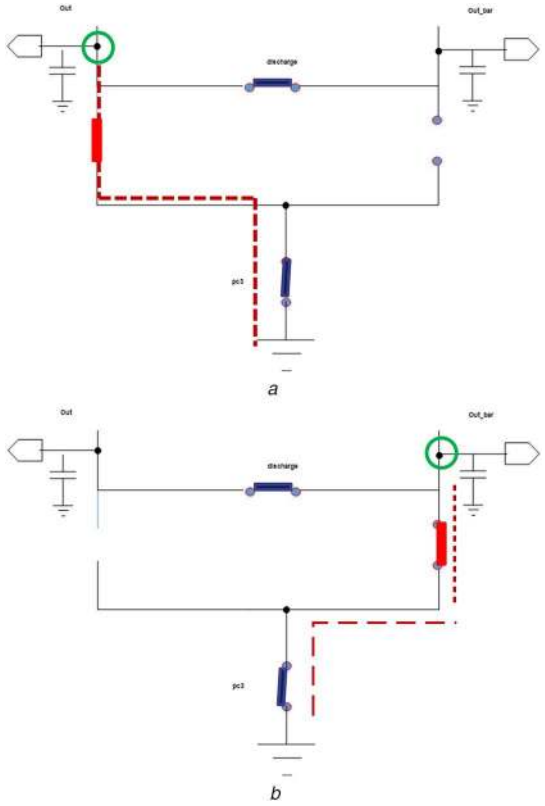

Fig. 11 *Discharge of unrecovered charge from output nodes*
(a) Not/buffer: In = 0, ***(b)*** Not/buffer: In = 1

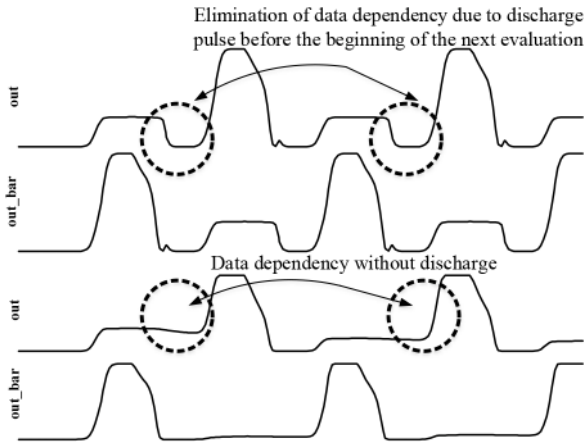

Fig. 12 *Elimination of data dependency*

supply and the ground is the lowest in the DCPAL family which is highlighted with the mention that DCPAL circuits realise lower leakage than the PFAL-based circuits [9, 19]. The leakage current values of CBSPAL and EE-SPFAL family have been calculated for constant inputs for individual logic operations through buffer/NOT, NAND/AND, and XOR/XNOR logic gates. Comparison of the leakage current values demonstrates that CBSPAL incurs lower leakage as highlighted in Table 3 while operating at a frequency of 12.5 MHz. Leakage current value of the proposed logic is 46% lower while driving a load capacitance of 10 fF and it is found to be 64% lower while driving a capacitive load of 50 fF. The reduction in leakage current makes this logic style more attractive for lightweight resource constrained applications.

Fig. 16 shows XOR/XNOR gate structures as employed for the proposed CBSPAL family. In the XOR/XNOR gate, M1 and M2 transistors have been used for charging and energy recovery operations between output capacitance and power clock PC1. M6_1, M6_2, M6_3, and M6_4 are the transistors used to discharge the additional charge stored in the load capacitors before evaluation of next state inputs are attempted. The remaining

Table 2 Comparison of the energy of buffers [32 nm]

Energy (aJ)	SYAL	SPGAL	EE-SPFAL	CBSPAL
1.25 MHz	11,500	7460	0.00956	0.00379
12.5 MHz	2250	1510	0.000178	0.00000178
125 MHz	792	1310	0.0000161	0.00000514

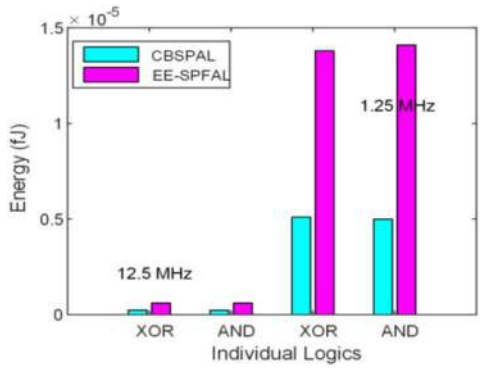

Fig. 13 *Comparison of energy consumption – XOR and AND gates*

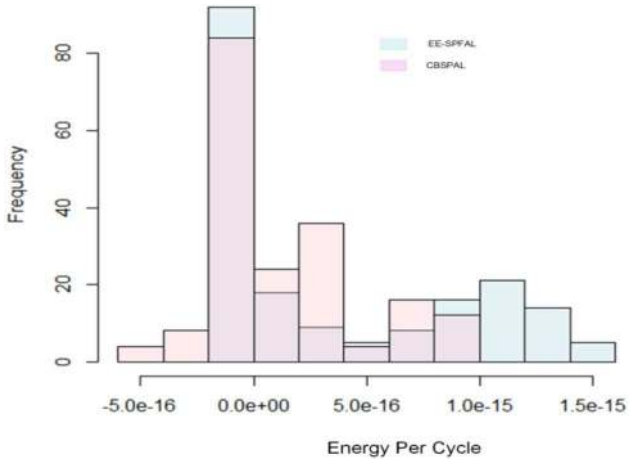

Fig. 14 *XOR/XNOR gates – energy distribution comparison at 1.25 MHz*

transistors are used for functional evaluation. AND/NAND gate follows a similar construction and the inputs are reordered as per the functional evaluation for the AND/NAND gate functionality. The pull down network is used for the functional evaluation in CBSPAL family. The discharge transistors and evaluation transistors have been arranged in a symmetric manner to balance load capacitance values. Table 4 indicates the number of transistors employed in each of the secure adiabatic logic for individual logic gate realisations. The normalised energy deviation (NED) and the normalised standard deviation (NSD) calculations estimate the energy uniformity of the proposed logic per cycle for various input transitions [24, 25]. The parameter NED is defined as (E_max–E_min)/E_max and is used to identify the percentage difference between the minimum E_min and maximum energy consumption E_max for all the possible transitions. The parameter NSD is defined as $\sigma\_E/\tilde{E}, \sigma E$ indicates the variation of the energy dissipation and $\tilde{E}$ is the average of energy dissipation of all the possible input transitions. The values of NED and NSD estimate the power analysis resistance of the circuit. Table 5 show the comparison among the NED and NSD values of the existing secure adiabatic logic families. NED of the CBSPAL is found to be very less and CBSPAL XOR gate exhibits only 0.2 and 0.5% of energy deviation at a frequency of 12.5 and 125 MHz, respectively. The calculated values of NED and NSD are observed to be less in comparison against the EE-SPFAL and SYAL styles and it reflects the ability of XOR/XNOR and AND/NAND gates against power analysis attacks. In addition, the energy deviation is less in the entire range of frequencies compared to the existing DPA resistant adiabatic logic families, which make the proposed logic more

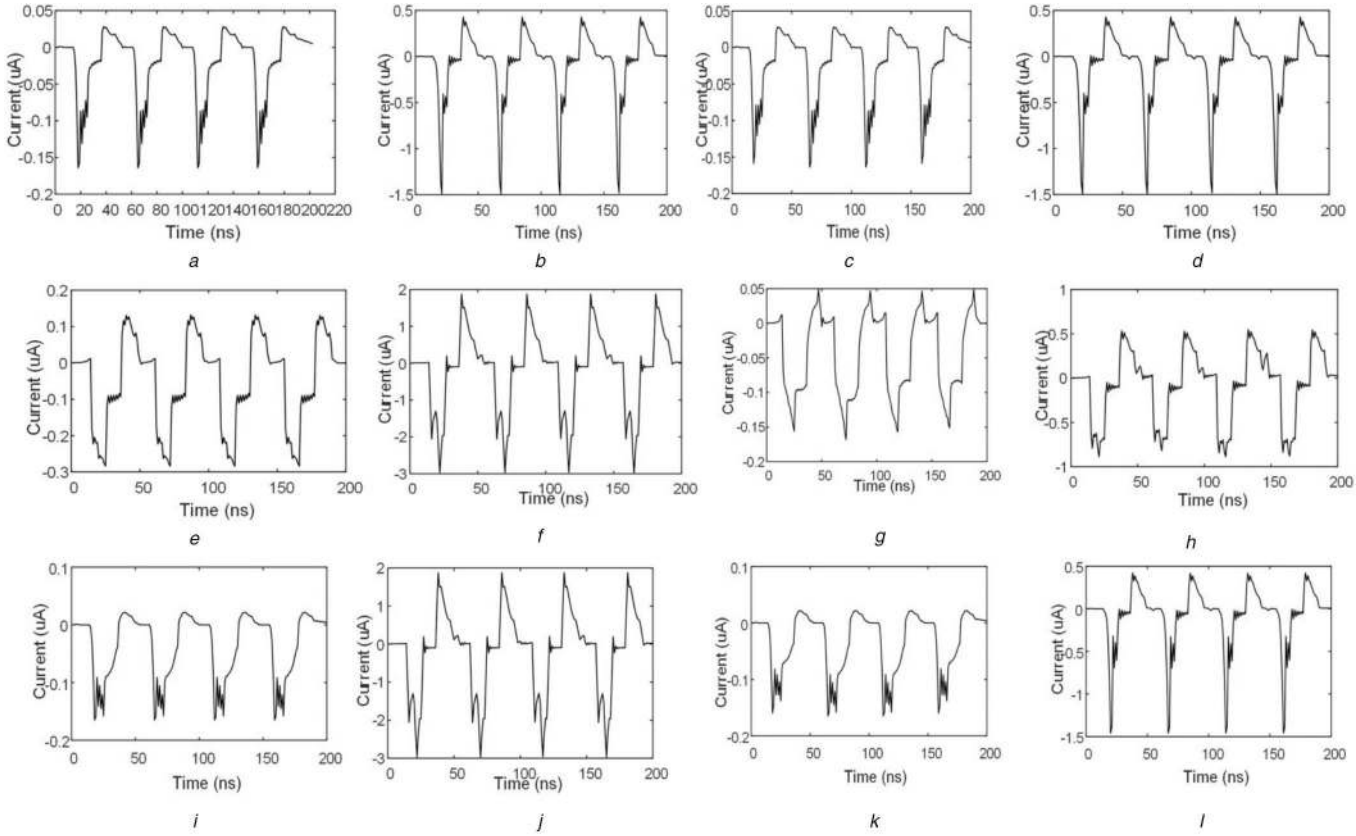

Fig. 15 *Supply trace for input patterns AB = 00, 01, 10 and 11 at 1.25 and 12.5 MHz*
(a)–(d) CBSPAL XOR and AND gate, ***(e)–(h)*** EE-SPFAL XOR and AND gate, ***(i)–(l)*** SYAL XOR and AND gate

Table 3 Leakage current comparison at 12.5 MHz

Logic family	C_L = 10 fF							C_L = 50 fF						
	$A=0$	$A=1$	$A=0$, $B=0$	$A=0$, $B=1$	$A=1$, $B=0$	$A=1$, $B=1$	Average current	$A=0$	$A=1$	$A=0$, $B=0$	$A=0$, $B=1$	$A=1$, $B=0$	$A=1$, $B=1$	Average current
EE-SPFAL, (nA)														
buffer\NOT	97.53	97.29	NA				97.41	138.59	138.47	NA				138.53
AND\NAND	NA		111.7	124.9	97.1	111.2	111.22	NA		154.8	167.73	139.72	154.82	154.26
XOR\XNOR	NA		111.32	111.04	111.06	111.32	111.18	NA		153.79	153.62	153.61	153.79	153.70
CBSPAL, (nA)														
buffer\NOT	42.92	42.34	NA				42.63	88.16	83.72	NA				85.94
AND\NAND	NA		50.52	51.51	51.52	50.52	51.01	NA		96.90	95.41	95.37	96.90	96.15
XOR\XNOR	NA		51.51	51.36	51.35	51.52	51.43	NA		95.41	94.49	95.53	95.37	95.20

NA, not applicable.

suitable for the design of secure low power hardware. The uniform supply current across the frequencies is also observed for the proposed AND/NAND and XOR/XNOR logic gates as shown in Section 4 and it additionally validates the power analysis robustness.

5 Analysis of the substitution permutation network (SPN) 4-bit add-round structure

The power analysis attack mechanisms proposed by Kocher *et al.*, serve as a well-established approach to evaluate the efficiency of the cryptosystems against DPA attacks [26, 27]. The different types of side channel power attack methods are the simple power analysis, the DPA and the CPA. Both the DPA- and the CPA-based power analysis attack mechanisms are effective in determining the robustness of power attacks. The power analysis attacks prominently concentrate on the dynamic power to reveal the secret information. Literature also reports leakage power attack schemes to hack the hidden information [28]

5.1 Substitution permutation network (SPN)

The CPS and the IOT motivate the deployment of lightweight cryptographic algorithms to offer security. Recent studies aim at the study of the trade-off between the performance and security estimation of the hardware and software implementation of lightweight cryptographic algorithms for IOT and CPS systems [29]. The lightweight block ciphers have two types of structures, namely, the SPN structure and the Feistel structure. The SPN structure employed in the lightweight block ciphers is shown in Fig. 17. The add-round key is the primary key mixing operation in the SPN type of ciphers. The add-round operation has been chosen to demonstrate the security efficiency of the proposed logic. Fig. 18 shows 4-bit add-round key architecture employed in this work. The 4-bit add-round block is provided with a common supply clock. CBSPAL employs four-phase trapezoidal power clocks which differ from each other by 90°, similar to that of the existing four-phase adiabatic logic styles. Every successive stage of the adiabatic pipeline is operated with the power clock phases PC1/PC3, PC2/PC4, PC3/PC1, and PC4/PC2. To implement the 4-bit add-round structure using the proposed logic, 64 transistors have been used. The static CMOS add-round structure employs 32 transistors for

the 4-bit add-round structure. The simulation results of 4-bit add-round operation using the proposed logic and the static CMOS logic incur average energy values of 0.922 zJ and 28.1231 nJ, respectively, while operating at 125 MHz.

5.2 CPA attack on add-round key circuit

The security evaluation of the proposed CBSPAL is made by the CPA attacks on 4-bit add-round architecture of the SPN structure implemented using the proposed logic. SPICE simulations have been carried out. CPA statistically analyses the power traces to extract the key information.

The CPA mechanism employed is summarised in Fig. 19. The steps necessary for identifying the secret key using CPA are described as follows [30]:

- *Description of target operation:* The first step in power analysis is to identify the target operation and its implementation under attack. In the context of this paper, we investigated the 4-bit add-round key architecture implementation of the SPN structure. The selection of the linear operation demonstrates the strength of the attack.
- *Selection of power consumption model:* The estimation of the hypothetical power model of the target operation under attack is

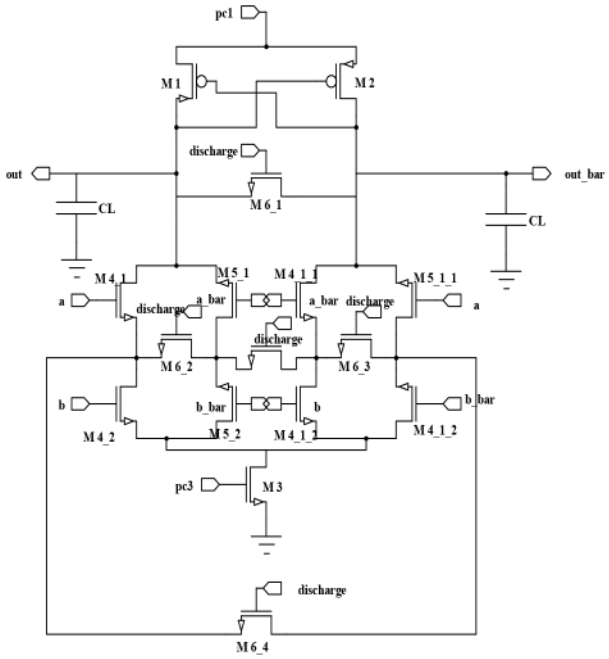

Fig. 16 *Proposed XOR/XNOR gate*

Table 4 Transistor count comparison

Adiabatic logic family	Logic gate	Transistor count per gate
EE-SPFAL [9]	BUFFER	8
	XOR	12
	AND	14
SPGAL [5]	BUFFER	6
	XOR	10
	AND	12
CSSAL [10]	BUFFER	11
	XOR	21
	AND	21
SYAL [2]	BUFFER	5
	XOR	15
	AND	15
CBSPAL [Proposed]	BUFFER	6
	XOR	16
	AND	16

Table 5 Simulation results of XOR/XNOR gate

LOGIC	Gate	12.5 MHz		125 MHz	
		NED	NSD	NED	NSD
EE-SPFAL [32 nm]	XOR	0.0007	0.0003	0.0017	0.0008
	AND	0.010	0.004	0.1249	0.0619
CBSPAL [32 nm]	XOR	0.0002	0.0009	0.0005	0.0002
	AND	0.003	0.0017	0.0011	0.0004
SYAL [32 nm]	XOR	0.0019	0.0011	0.0016	0.0006
	AND	0.0351	0.0204	0.7716	0.8456

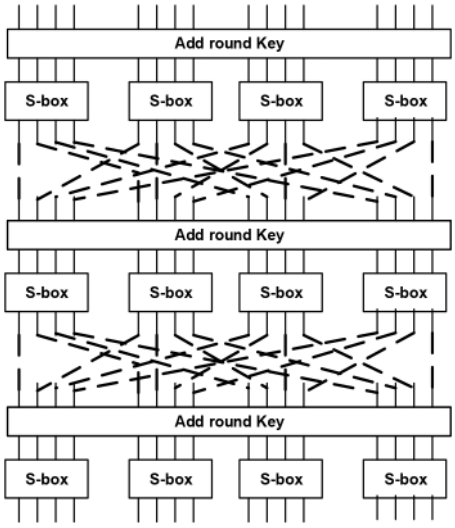

Fig. 17 *SPN structure*

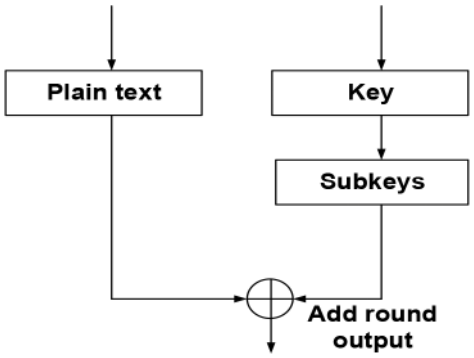

Fig. 18 *SPN add-round key architecture*

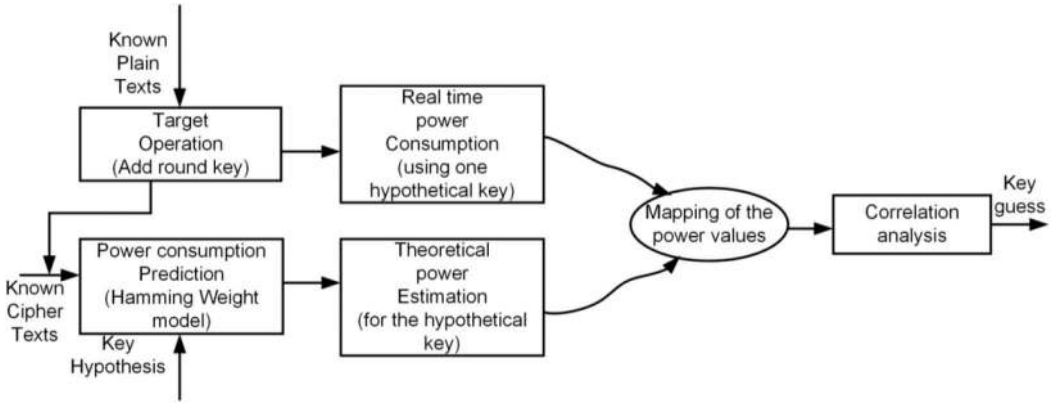

Fig. 19 *Correlation power attack mechanism*

the main criterion for the power attacks. These power estimations have been compared with real-time power consumption values that reveal the secret key information. The quality of the predicted model decides the effectiveness of the attack. The power consumption estimation is based on the main hypothesis that power consumption is proportional to the number of bit transitions.

- *Prediction of device power consumption:* Prediction of power consumption of the selected function is made using hypothetical keys. The expected outputs are recorded along with the power values. Let I_i represent an element in the set of plain text I where $i \in [0, d-1]$ and d is the number of plain texts. Let K represent the set of hypothetical keys and K_j be the element in K where $j \in [0, k-1]$, where k is the total number of possible keys for the test circuit. The total numbers of possible keys are $2^4 = 16$ for the 4-bit add-round structure. The output cipher text O has the element $O_{i,j}$ given by

$$O_{i,j} = (I_i \text{ XOR } K_j)$$

The Hamming weight $H(O_{i,j})$ of the output cipher text serves as the hypothetical power model for the power analysis attack and is expressed as

$$H(O_{i,j}) = H((\text{input}) \text{ XOR key}))$$

- *Measurement of device power consumption*: The power traces are recorded for different input plain texts. For every simulation, the power traces have been collected and recorded for the targeted clock cycle. Every plain text is encrypted using a unique secret key. As a result of the measurement phase, the attacker obtains 16×1 cipher texts with their power consumption values for 16 different plain texts. This 16×1 power consumption matrix is the global consumption vector.
- *Correlation analysis:* As a final phase, the theoretical power predictions are compared with its real measurements at different

uniform instances of time over the targeted clock cycle. The correlation coefficient is computed between the global consumption vector and all the columns of the power estimation matrix. For the successful key guess, a high correlation value will result when the power prediction is accurate.

Let N_i denote the ith measurement trace and N the set of traces. Let P_i denote power prediction for the ith trace and P the set of predictions. Then

$$C(N,P) = \frac{\mu_{N\cdot P} - \mu_N \cdot \mu_P}{\sigma_N \cdot \sigma_P}$$

where μ_N is the mean of the traces N and σ^2 is its variance.

The attacker identifies the maximal value in the correlation matrix. For the successful CPA attack, the correlation value will be high if the prediction model and the key hypothesis happen to be accurate.

5.3 Results and discussion

The CPA attack is performed on CBSPAL, EE-SPFAL, and static CMOS style test circuits. There are no noises in the measurement set up and the real-time ideal test environment is considered for the CPA attack platform. There are no additional analogues or digital modules associated with the system. Static CMOS style, EE-SPFAL, and CBSPAL implementation follow the same environment. The CPA attack is performed in 4-bit add-round key operation of a SPN with the key $(1010)_2$. The test circuitry is an add-round key operation which consists of 4 XOR gates fed by a common supply clock. The plain texts are fed to the test circuitry and their real-time power traces have been recorded. The testing of the design is performed at 40,000 different time instants to reveal the secret key. The static CMOS and EE-SPFAL style implementation revealed the secret key in a few number of power traces. The correlation coefficient graph of the static CMOS logic for attempt on the correct key guess using the CPA analysis is shown in Fig. 20. The high-correlation factor reflects the highly probable key and the maximum possible correlation value is 1. The add-round operation is a linear operation and the correlation coefficient value is high for the keys $(1010)_2$ and $(0101)_2$, respectively, for the static CMOS implementation.

The CBSPAL implementation does not reveal the correct key even after the CPA-based tests in 40,000 different timing instants. The peak correlation coefficient value for the CBSPAL add-round test circuit is value of 0.2 for the wrong key $(1001)_2$ and it shows the effectiveness of the proposed logic against power attacks. It can be observed from Fig. 20 that the correct key is hidden in CBSPAL implementation, with a very less correlation value of 0.304×10^{-4}. The signal-to-noise ratio (SNR) is also a useful measurement to predict the power analysis robustness. It indicates the marginal probability for the correct key prediction between the successive key guesses. The difference in SNR value between the first high key guess correlation and the second high correlation value of the CBSPAL implementation is also less.

The security characteristics of the CBSPAL logic are additionally validated by plotting the supply current trace and the supply power trace in the frequencies ranging from 1.25 to 125 MHz. Figs. 21*a–c* show the respective supply current traces and supply power traces at 1.25, 12.5, and 125 MHZ, respectively, and they show a uniform profile and thus the proposed logic is immune to power analysis attacks across the frequencies. The traces are recorded by considering random input data transitions and thus the CBSPAL logic is data independent also, which is an essential property for the security applications as mentioned in earlier sections. The NED and the NSD are the parameters that will reflect the security strength. As presented in Table 6, the add-round test circuit exhibits very low energy deviation and low standard deviation for the range of frequencies from 1.25 to 125 MHz.

The energy consumption of the test circuit using CBSPAL logic is recorded across the range of frequencies and the results are compared with the static CMOS style-based test circuit. For fairer

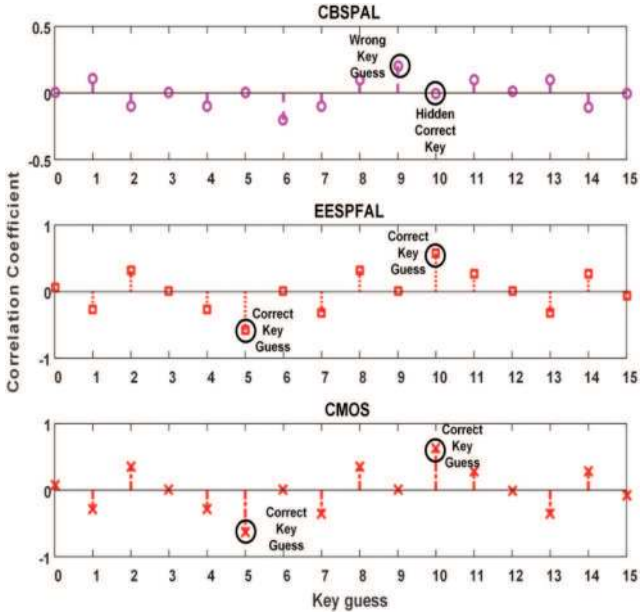

Fig. 20 *CBSPAL non-successful CPA attack*

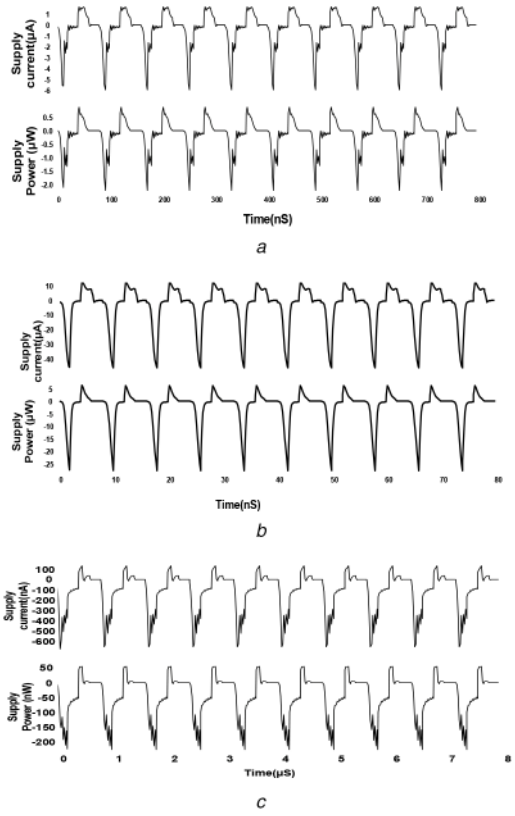

Fig. 21 *Supply current and supply power trace of CBSPAL add-round key circuit*
(a) 1.25 MHz, ***(b)*** 12.5 MHz, ***(c)*** 125 MHz

Table 6 Security evaluation of add-round key operation

Logic style/frequency	Static CMOS	CBSPAL
NED		
1.25 MHz	0.258692	0.001327
12.5 MHz	0.258677	0.001209
125 MHz	0.076712	0.000315
NSD		
1.25 MHz	0.076717	0.000408
12.5 MHz	0.258676	0.00151
125 MHz	0.076712	0.000503

Table 7 Add-round key test area comparison

Logic family	No. of. transistors
static CMOS	64
CBSPAL	32

Table 8 Energy consumption of add-round key test circuit

Energy consumption/ frequency	Static CMOS	EE-SPFAL	CBSPAL
12.5 MHz	28.1231 fJ	0.933 zJ	0.922 zJ
125 MHz	28.1231 nJ	50 zJ	0.14 zJ

comparisons, both the CMOS and the CBSPAL circuits were implemented in the same platform. The proposed logic incurs 50% additional area overhead than the static CMOS logic as shown in Table 7 and it saves up to 89.5% energy than the static CMOS logic.

Across the various frequency ranges, it is observed from Table 8 that energy efficiency of the proposed logic improves as frequency increases.

6 Conclusion

A novel CBSPAL resistant to power analysis attacks is proposed. The mechanisms incorporated in the proposed logic to improve the performance and security strength are adiabatic logic for low power capabilities using the principle of charge recovery, unique power clocking mechanism to pre-resolve the output nodal capacitance to zero which result in reduced non-adiabatic loss, symmetric charge balancing structure to have uniform supply current consumption and discharging the unrecovered charge before the beginning of every evaluation to eliminate the input data dependency. Area overhead of the proposed logic is 50% more than the static CMOS implementation. However, the area consumption is on par with the existing secure adiabatic logic styles and less than the CMOS-based secure logic styles. The inheritance of these mechanisms offers increased energy efficiency and removes data independence between the successive evaluations. The simulation results validate the energy efficiency of the proposed logic. The energy efficiency of the proposed CBSPAL logic outperforms the existing secure adiabatic logic families and the static CMOS logic. The security strength of the proposed logic is also proven through a similar set of security analysis in the existing literature.

7 References

[1] Song, H., Fink, G.A., Jeschke, S. (Eds.): '*Security and privacy in cyber-physical systems: foundations, principles, and applications*' (John Wiley & Sons, Hoboke, NJ, USA, 2017)

[2] Choi, B.-D., Kim, K.E., Chung, K.-S., *et al.*: 'Symmetric adiabatic logic circuits against differential power analysis', *ETRI J.*, 2010, **32**, (1), pp. 166–168

[3] Monteiro, C., Takahashi, Y., Sekine, T.: 'Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks'. 36th Int. Conf. on Telecommunications and Signal Processing (TSP), Rome, Italy, 2013, pp. 732–736

[4] Avital, M., Dagan, H., Levi, I., *et al.*: 'DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes', *IEEE Trans. Circuits Syst. I, Regul. Pap.*, 2015, **62**, (1), pp. 149–156

[5] Kumar, S.D., Thapliyal, H., Mohammad, A., *et al.*: 'Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware', *Integr. VLSI J.*, 2016, **58**, pp. 369–377

[6] Morrison, M., Ranganathan, N.: 'Synthesis of dual-rail adiabatic logic for low power security applications', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2014, **33**, (7), pp. 975–988

[7] Morrison, M.A., Ranganathan, N., Ligatti, J.: 'Design of adiabatic dynamic differential logic for DPA-resistant secure integrated circuits', *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 2015, **23**, (8), pp. 1381–1389

[8] Kumar, S.D., Thapliyal, H., Mohammad, A.: 'FinSAL: FinFET based secure adiabatic logic for energy-efficient and DPA resistant IoT devices', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2018, **37**, (1), pp. 110–122

[9] Kumar, S.D., Thapliyal, H., Mohammad, A.: 'EE-SPFAL: a novel energy-efficient secure positive feedback adiabatic logic for DPA resistant RFID and smart card', *IEEE Trans. Emerg. Top. Comput.*, 2016, **7**, pp. 281–293

[10] Monteiro, C., Takahashi, Y., Sekine, T.: 'Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level', *Microelectron. J.*, 2013, **44**, (6), pp. 496–503

[11] Raghav, H., Bartlett, V., Kale, I.: 'Robustness of power analysis attack resilient adiabatic logic: WCS-QuAL under PVT variations', 2017 27th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS), Thessaloniki, Greece, 2017

[12] Moradi, A., Poschmann, A.: 'Lightweight cryptography and DPA countermeasures: a survey'. Financial Cryptography Workshops, Canary Islands, Spain, 2010, pp. 68–79

[13] Bi, Y., Shamsi, K., Yuan, J.-S., *et al.*: 'TUNNEL FET current mode logic for DPA-resilient circuit designs', *IEEE Trans. Emerg. Top. Comput.*, 2017, **5**, (3), pp. 340–352

[14] Bucci, M., Giancane, L., Luzzi, R., *et al.*: 'Three-phase dual-rail pre-charge logic'. Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES), Yokohama, Japan, 2006, vol. 4249, pp. 232–241

[15] Guilley, S., Sauvage, L., Flament, F., *et al.*: 'Evaluation of power constant dual-rail logics countermeasures against DPA with design time security metrics', *IEEE Trans. Comput.*, 2010, **59**, (9), pp. 1250–1263

[16] Moradi, A., Shalmani, M.T.M., Salmasizadeh, M.: 'Dual-rail transition logic: a logic style for counteracting power analysis attacks', *Comput. Electr. Eng.*, 2009, **35**, (2), pp. 359–369

[17] Akkaya, N.E.C., Erbagci, B., Carley, R., *et al.*: 'A DPA-resistant self-timed three-phase dual-rail pre-charge logic family'. 2015 IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST), Washington DC, USA, 2015, pp. 112–117

[18] Tena-Sanchez, E., Castro, J., Acosta, A.J.: 'A methodology for optimized design of secure differential logic gates for DPA resistant circuits', *IEEE J. Emerg. Sel. Top. Circuits Syst.*, 2014, **4**, (2), pp. 203–215

[19] Bhaaskaran, V.S., Raina, J.P.: 'Differential cascode adiabatic logic structure for low power', *J. Low Power Electron.*, 2008, **4**, (2), pp. 178–190

[20] Bhaaskaran, K.: 'Dynamic pre-resolve charge recovery logic'. 2014, Patent No. 883/ CHE/2011A

[21] Bhaaskaran, V.S.K.: 'Energy recovery performance of quasi-adiabatic circuits using lower technology nodes'. Int. Conf. on In Power Electronics (IICPE), New Delhi, India, 2011, pp. 1–7

[22] Kanchana Bhaaskaran, V.S., Raina, J.P.: 'Pre-resolve and sense adiabatic logic for 100 KHz to 500 MHz frequency classes', *J. Circuits Syst. Comput.*, 2012, **21**, (5), pp. 1250045

[23] 'PTM 32 nm HSPICE Model'. Available at http://ptm.asu.edu/modelcard/HP/22nm_HP.pm, accessed 15 December 2017

[24] Wu, J., Shi, Y., Choi, M.: 'Measurement and evaluation of power analysis attacks on asynchronous S-box', *IEEE Trans. Instrum. Meas.*, 2012, **61**, (10), pp. 2765–2775

[25] Bi, Y., Shamsi, K., Yuan, J.-S., *et al.*: 'Emerging technology-based design of primitives for hardware security', *J. Emerg. Technol. Comput. Syst.*, 2016, **13**, (1), pp. 3:1–3:19

[26] Alioto, M., Poli, M., Rocchi, S.: 'A general power model of differential power analysis attacks to static logic circuits', *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 2010, **18**, (5), pp. 711–724

[27] Kocher, P., Jaffe, J., Jun, B.: 'Differential power analysis'. Advances in Cryptology—CRYPTO'99, Santa Barbara, CA, USA, 1999, pp. 789–789

[28] Alioto, M., Bongiovanni, S., Djukanovic, M., *et al.*: 'Effectiveness of leakage power analysis attacks on DPA-resistant logic styles under process variations', *IEEE Trans. Circuits Syst. I, Regul. Pap.*, 2014, **61**, (2), pp. 429–442

[29] McKay, K.A., Bassham, L., Turan, M.S., *et al.*: 'Report on lightweight cryptography'. NIST DRAFT NISTIR 8114, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, 2016

[30] Standaert, O.-X., Peeters, E., Rouvroy, G., *et al.*: 'An overview of power analysis attacks against field programmable gate arrays', *Proc. IEEE*, 2006, **94**, (2), pp. 383–394