Symmetric Power Analysis Attack Resilient Adiabatic Logic for Smartcard Applications

Raghav, H. and Kale, I.

Symmetric Power Analysis Attack Resilient Adiabatic Logic for Smartcard Applications

Himadri Singh Raghav and Izzet Kale
Applied DSP and VLSI Research Group, Department of Engineering
University of Westminster
Email: himadri.s.raghav@my.westminster.ac.uk, kalei@westminster.ac.uk

***Abstract*—On the whole existing secure adiabatic logic designs exhibit variations in current peaks and have asymmetric structures. However, asymmetric structure and variations in current peaks make the circuit vulnerable to Power Analysis Attacks (PAA). In this paper, we shall present a novel PAA resilient adiabatic logic which has a symmetric structure and exhibits the least variations in current peaks for basic gates as well as in 8-bit Montgomery multiplier. The proposed logic has been compared with two recently proposed secure adiabatic logic designs for operating frequencies ranging from 1MHz to 100MHz and power-supply scaling ranging from 0.6V to 1.8V. Simulation results of the gates show that our proposed logic exhibits the lowest Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) under the said frequency variations. All the 2-input gates that deploy the proposed logic dissipate nearly the same average energy within 0.2% of each other at all the frequencies simulated and thus, along with the data-independence, gate-function-independence is achieved. The paper will also report on the energy dissipated by the proposed logic which approaches that of the existing logic designs as the output load capacitance is increased above 100fF. The simulation results of the 8-bit adiabatic Montgomery multiplier show that the proposed logic exhibits the least value of NED and NSD under the said frequency variations and power-supply scaling. Finally, the paper will report on the current waveform graphs for variations in current peaks under power-clock scaling.**

Keywords— power analysis attacks resilient; secure adiabatic logic; charge sharing; energy consumption; countermeasure

I. INTRODUCTION

Smartcards today are used in a wide variety of applications such as banking, access control, transport, electronic commerce and many others. In all these applications, the security of the information stored on the smartcard is of utmost importance. Cryptography algorithms are used to protect the secret information stored on the smartcards. However, the hardware implementation of the cryptography algorithms is susceptible to Power Analysis Attacks (PAA).

In PAA, the attacker attempts to expose the secret information such as the secret key, by monitoring the power supply currents during the execution of the critical operations such as encryption and decryption. By monitoring the power-supply currents, the secret key used in the cryptographic device can and may be inferred. Therefore, to make the cryptographic device resistant to PAA, the power consumption of the cryptographic device should be made independent of the input data.

Several countermeasures have been proposed in the open literature to make the cryptographic implementations secure against PAA and are employed at the cell (gate) level. Hiding [2] and masking [3] are the countermeasures generally applied at the gate level. The objective of hiding is to make the power consumption of the cryptographic device data-independent whereas, masking relies on randomizing the input/key dependent intermediate values processed in the cryptographic device. This makes the power consumption of the cryptographic device mostly independent of the actual intermediate values.

This paper is organized as follows; in section II, the background of the PAA resilient adiabatic logic is presented. The existing logic designs and their shortcomings are discussed in section III. The proposed logic is presented in section IV. In section V, simulation results are presented, and finally, the paper is concluded with section VI.

II. BACKGROUND

The logic design approaches such as Charge-Sharing Symmetric Adiabatic Logic (CSSAL) [4], Symmetric Adiabatic Logic (SyAL) [5], Secure Quasi-Adiabatic Logic (SQAL) [6], Symmetric Pass Gate Adiabatic Logic (SPGAL) [9] and Energy Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) [10] are the existing secure adiabatic logic approaches resilient to PAA.

For warranting data-independent energy dissipation, these adiabatic design approaches use the charge-sharing technique at the output/internal nodes and load balancing at the two output nodes. SyAL and SQAL are based on Efficient Charge Recovery Logic (ECRL) [7]. CSSAL, on the other hand, is based on 2N-2N2P adiabatic logic [8] and is an improvement over SyAL. SPGAL and EE-SPFAL are the recently proposed secure adiabatic approaches that are proved to be better in comparison to CSSAL, SyAL, and SQAL based on %NED and %NSD. Therefore, a comparison of the performance between the proposed logic, SPGAL and EE-SPFAL based on %NED and %NSD, energy dissipation and variations in current peaks is presented in this paper.

To further evaluate and compare the performance of the proposed logic, an 8-bit Montgomery multiplier based on the radix-2 Montgomery multiplication algorithm reported in [13] was implemented as a vehicle to investigate the impact of frequency variations, power supply scaling on %NED, %NSD and current peak variations.

III. EXISTING LOGIC DESIGNS AND THEIR LIMITATIONS

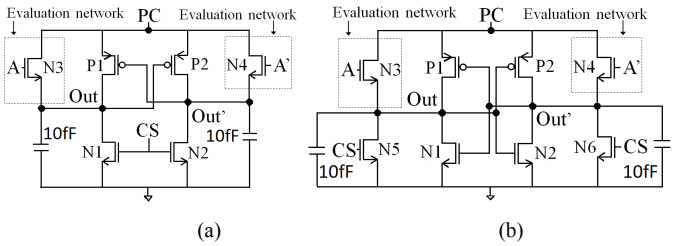


Fig. 1. NOT/BUF gate (a) SPGAL[9] (b) EE-SPFAL[10].

The schematic of the SPGAL NOT/BUF gate is shown in Fig. 1(a). The structure of SPGAL suffers from severe coupling effect due to the absence of cross-coupled nMOS transistors. It is because when one of the output nodes follows the PC, the complementary node gets coupled to it during evaluation, hold, and recovery phase of the power-clock, leading to sever coupling effect. This results in the complementary node voltage to rise above the threshold voltage (V_{tn}).

The schematic shown in Fig. 1 (b) is that of the NOT/BUF gate using EE-SPFAL. Unlike SPGAL, EE-SPFAL, due to the presence of cross-coupled nMOS transistors, N1 and N2, the two output nodes remain floating only for the part of the recovery phase when the PC falls below the threshold voltage of the pMOS transistor and therefore, suffers from coupling effect only for the part of the recovery phase of the power-clock.

Fig. 2 (a), (b) and (c) shows the schematic of the AND/NAND gate using SPGAL, EE-SPFAL and their equivalent RC models of the internal nodes during evaluation phase for 4 input combinations respectively. The equivalent RC models for AND/NAND gate using SPGAL and EE-SPFAL are same as both the secure logic are based on Positive Feedback Adiabatic Logic (PFAL) [11].

For having a symmetric structure two conditions should be fulfilled: 1) for each input combination/transition, an equal number of transistors should be ON at the two output nodes. 2) Even if the equal number of transistors is ON at the two output nodes, it should be ensured that the capacitance and the resistance on the two output nodes are same or the two output nodes charge the same capacitance for each input combination/transitions. From Fig. 2 (c), for input combinations AB='00' and '11' the two output nodes have a different number of transistors ON at the two output nodes, 'AND' and 'NAND'. For input combinations AB='01' and '10', seemingly two transistors are ON at the two output nodes, however, for input combination AB='01', output node, 'AND' has two ON transistors in parallel whereas, on the output node, 'NAND' the two ON transistors are in series. Similarly, for the input combination, AB='10', the output node, 'AND' has no ON transistors connected to it, instead the two ON transistors are connected to the power-clock (PC). On the output node, 'NAND' the two ON transistors are in series. This suggests that for each input combination the capacitance at the two output nodes is different leading to data-dependent behavior and an asymmetric structure. This makes the logic designs vulnerable to PAA.

IV. PROPOSED LOGIC WITH SINGLE CHARGE-SHARING

In order to achieve data-independent power consumption, the two output nodes of the adiabatic gate should charge equal capacitance (equal number of 'ON' transistors) for each input transitions. This is achieved by having a symmetric structure, where an equal number of transistors are turned 'ON' at the two output nodes for each input transition. To achieve this, our proposed logic is implemented using a dual duplicate evaluation network, one connected between the power-clock and the two output nodes and the other connected between the two output nodes and ground as shown in Fig. 3(a). This guarantees an equal number of transistors to be ON at the diagonally opposite evaluation networks on the two output nodes for each input transition. Having dual duplicate evaluation network helped to make the circuit symmetric and to get the data-independent power-consumption. It also helps the two output nodes to discharge to zero before the evaluation of the next inputs.

The schematic of the NOT/BUF gate using proposed logic, its simulation results at 10MHz and the current peaks for 4 input transitions of the NOT/BUF gate respectively are shown in Fig. 3(a), (b) and (c). The charge during the idle phase of the PC when the inputs have not yet reached the threshold voltage of the transistors is shared by the charge sharing transistor. It also connects the two output nodes to the ground before the evaluation of the next inputs. Charge sharing transistor uses

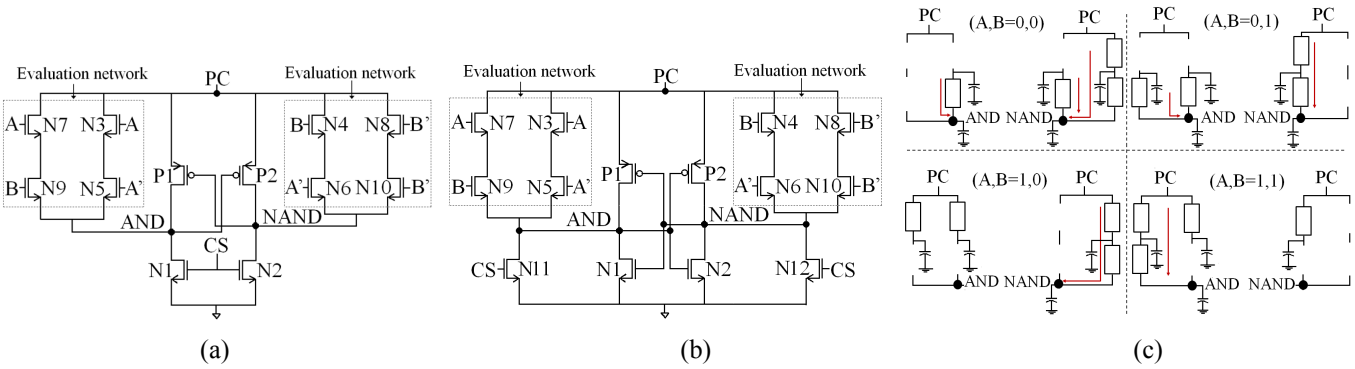


Fig. 2. AND/NAND gates (a) SPGAL[9] (b) EE-SPFAL [10](c) Equivalent RC models of SPGAL/EE-SPFAL.

a clock signal having 25% duty cycle with steeper rise and fall time. The operation of the proposed logic is described taking an example of a NOT/BUF gate. N3, N4, N5, and N6 are the input transistors, and P1, P2, N1 and N2 forms the cross-coupled latch responsible for holding the output nodes to their respective voltages and N7 is the charge sharing transistor. The simulation result shows the PC, Charge Sharing input, CS, input A, its complement A', and the complementary output nodes (Out, Out'). Fig. 3 (c) shows the PC, input A, charge sharing input, CS, and current peaks for 4 input transitions.

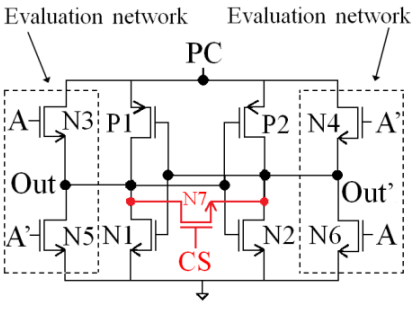
The operation is explained for A= '1', A'= '0'.

During the Idle phase (I) when input A is ramping up, transistors N3 and N6 are turned ON after they reach the threshold voltage. Also, the charge sharing transistor N7 is turned ON. The charge sharing transistor warrants that both the output nodes have the same charge for the interval, the inputs are not ON. When transistors N3 and N6 are turned ON, the input transistor, N3 connects the output node, Out to PC (which is at logic '0') and makes it zero. Also, transistor N6 causes the output node, Out' to connect to ground. Additionally, transistor N7 is connected between the two output nodes thus; both the output nodes are discharged to '0' before the evaluation of the next input.

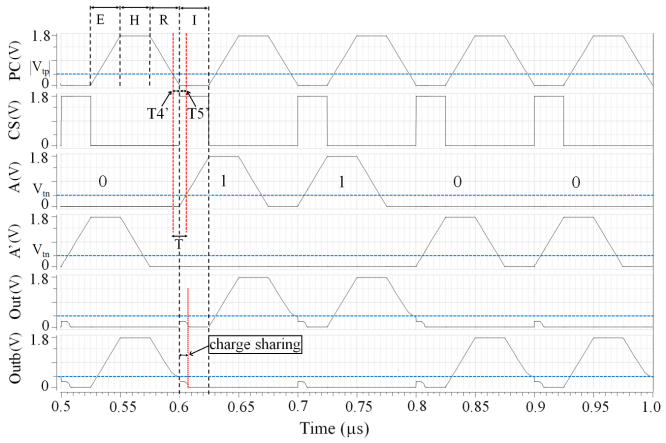
During the Evaluation phase (E), input A is logic '1' (A' is logic '0') and the PC ramps up. The output node Out follows the PC through transistors, N3 and P1 from 0 to V_{DD}-V_{tn} and V_{tp} to V_{DD} respectively.

During the Hold phase (H), input, A ramps down and the transistors N3 and N6 are switched OFF when the gate-to-source voltage falls below the threshold voltage, V_{tn}. The two output nodes are held at their respective voltages due to the cross-coupled transistors (P1, P2, N1, and N2)

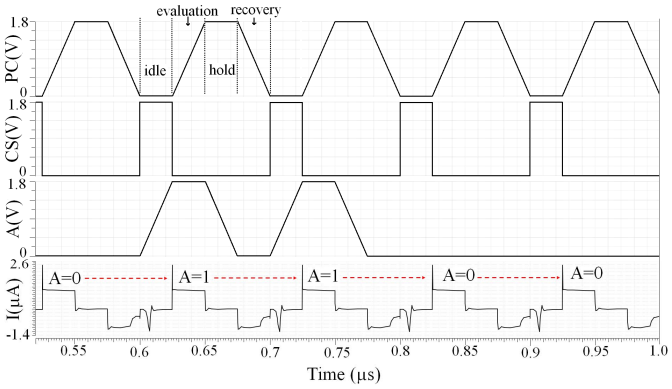
During the Recovery phase (R), the PC ramps down and the charge on the output node Out is recovered back to the PC through the transistor, P1. The charge is recovered till the PC falls below the threshold voltage, $|V_{tp}|$ of P1. At the time, T4', P1 is turned off and the node Out stays at V_{tp}. The leftover charge will be discharged to ground in the idle phase when the charge sharing transistor is turned ON and the next input arrives, and its gate voltage exceeds the threshold voltage (V_{tn}). From Fig. 3 (c) It can be seen that our proposed logic exhibits nearly same current peaks for all the 4 input transitions.



(a)



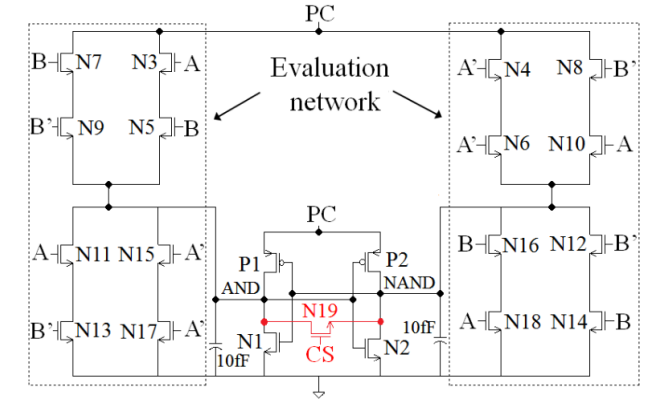
(b)



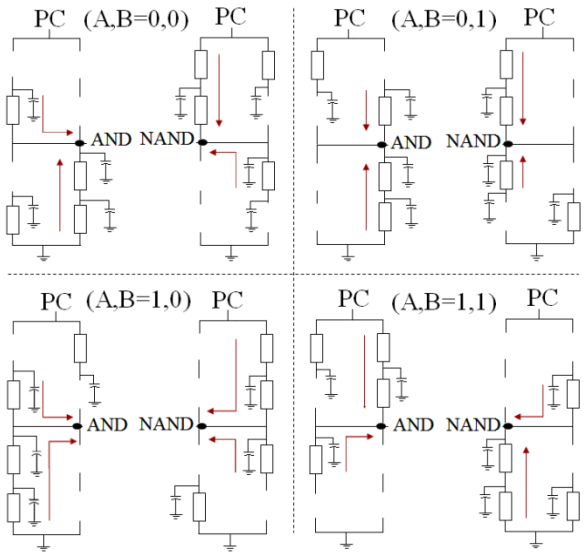
(c)

Fig. 3. (a) Proposed logic NOT/BUF gate (b) simulation result at 10MHz (c) Current peaks for 4input transitions.

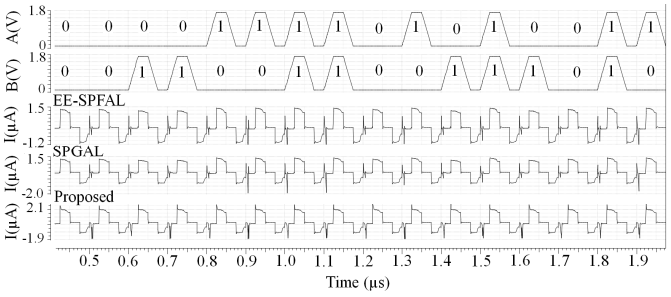
The schematic shown in Fig. 4 (a), and (b) is that of AND/NAND, gate using the proposed logic and its equivalent RC models for their internal nodes for 4 input combinations during the evaluation phase respectively. It can be seen that the two conditions for having a symmetric structure are fulfilled by the proposed logic 1) for each input combination, there is an equal number of ON transistors at the two output nodes. 2) For each input combination, it is ensured that the capacitance and the resistance on the two output nodes are same or the two output nodes charge the same capacitance. From Fig. 4 (b), for input combinations, AB='00', '11', '01', and '10' the two output nodes have 4 transistors ON and the same capacitance value is charged at the two output nodes leading to symmetric structure and data-independent behavior, unlike SPGAL and EE-SPFAL. All the 2-input logic gates implemented using the proposed logic have the same structure and an equal number of transistors, except the positions of the input signals.



(a)



(b)



(c)

Fig. 4. Proposed Logic (a) AND/NAND gate (b) Equivalent RC models (c) Current waveforms for 16 input transitions of AND/NAND gate using EE-SPFAL, SPGAL and the proposed logic at 10MHz

The simulation results shown in Fig. 4 (c) are the current waveforms for 16 input transitions of AND/NAND gate using the EE-SPFAL, SPGAL and the proposed logic. The complementary signals, A' and B' for AND/NAND are not shown for simplicity but follows adiabatic principle. The current waveforms are given for a power-clock frequency of 10MHz at 1.8V power-supply. The proposed logic exhibits the minimal variations in the current waveform compared to the existing logic design approaches, EE-SPFAL, SPGAL for all the input transitions.

V. Simulation Results

Simulations for the secure adiabatic approaches were performed with the Spectre simulator using Cadence EDA tool in a 'typical-typical', process corner using TSMC 180nm CMOS process at the 1.8V power supply. The simulations were performed at load capacitance of 10fF and the transistor sizes for all the designs were set at the technology minimum ($W_{min}=W_n=W_p=220$nm, $L_{min}=L_n=L_p=180$nm). The simulations were carried at frequencies 1MHz, 10MHz and 100MHz. The energy dissipation per cycle was measured for all the possible input transitions for NOT/BUF and 2-input gates for the proposed logic, SPGAL, and EE-SPFAL. To evaluate the resistance of proposed logic, SPGAL, and EE-SPFAL against PAA, Normalised Energy Deviation (NED) and Normalised Standard Deviation (NSD), are obtained according to (1) and (2). Where, E_{max}, E_{min}, E_{av}, and σ are maximum energy, minimum energy, average energy and standard deviation respectively. The smaller the difference between the maximum and minimum energy values the smaller the %NED and %NSD and lower the cell's vulnerability to PAA.

The Normalised Energy Deviation (NED) is defined as:

$$NED = (E_{max} - E_{min})/E_{max} \quad (1)$$

Normalized Standard Deviation (NSD) [12] is defined as:

$$NSD = \sigma/E_{av} \quad (2)$$

Standard Deviation is defined as:

$$\sigma = \sqrt{\sum_{i=1}^{En}(E_i - E_{av})^2}\Big/n \quad (3)$$

A. Impact of Frequency Variations

The simulation results of the evaluated gates using the proposed logic, SPGAL and EE-SPFAL at 1MHz, 10MHz and 100MHz are summarised in Table I. on the basis of %NED and %NSD, the performance of the proposed logic is the best as it exhibits the least value of %NED and %NSD followed by EE-SPFAL and SPGAL at all simulated frequencies. Table I also shows that the energy dissipation of proposed logic for 2-input gates is greater than SPGAL and EE-SPFAL at all simulated frequencies. It is because the proposed logic uses a dual duplicate evaluation network and thus have high internal node capacitance than SPGAL and EE-SPFAL. At lower values of load capacitances, the load at the output nodes of proposed logic will largely be dominated by its internal load capacitance and thus dissipate more energy.

TABLE I. SIMULATION RESULTS COMPARING THE %NED OF NOT/BUF, AND/NAND, OR/NOR AND XOR/XNOR GATES.

Logic Gates	1 MHz			10 MHz			100MHz		
	[9]	*[10]*	*Proposed*	*[9]*	*[10]*	*Proposed*	*[9]*	*[10]*	*Proposed*
NOT/BUF									
E_{av} (fJ)	1.755	1.792	1.867	2.387	2.455	2.538	5.352	5.725	5.710
%NED	1.920	0.501	0.267	0.209	0.406	0.393	0.816	0.400	0.279
%NSD	0.725	0.255	0.104	0.114	0.147	0.176	0.365	0.174	0.122
AND/NAND									
E_{av} (fJ)	5.740	5.772	5.869	6.053	6.170	6.459	9.602	9.787	10.690
%NED	9.800	6.756	0.458	7.969	6.320	0.139	7.672	6.168	0.186
%NSD	2.355	2.290	0.111	1.992	2.460	0.033	1.843	3.163	0.093
OR/NOR									
E_{av} (fJ)	4.784	5.028	5.868	5.116	5.506	6.458	8.027	8.648	10.692
%NED	9.457	7.961	0.509	7.094	5.938	0.123	6.668	3.913	0.187
%NSD	4.722	3.233	0.119	3.705	2.647	0.061	1.698	1.099	0.076
XOR/XNOR									
E_{av} (fJ)	3.328	3.529	5.870	3.908	4.138	6.460	7.390	8.027	10.691
%NED	1.430	0.537	0.508	0.127	0.096	0.030	0.607	0.174	0.186
%NSD	0.310	0.146	0.137	0.057	0.024	0.007	0.148	0.062	0.050

B. Logic Operation Independent Energy Disspation

The data shown in the Table II is of the average energy dissipation for all possible input transitions of 2-input gates (AND/NAND, OR/NOR and XOR/XNOR) implemented using SPGAL, EE-SPFAL, and the proposed logic. The Table also shows the standard deviation (σ) of average energy dissipated by AND/NAND, OR/NOR and XOR/XNOR using the existing and the proposed approach at all frequencies simulated. It can be seen that 2-input gates implemented using the proposed logic consume nearly same energy at all simulated frequencies and therefore, exhibits the least value of standard deviation than SPGAL and EE-SPFAL. This acts as an additional level of protection by guaranteeing, as far as possible, that all the 2-input gates use the same energy; thereby making it difficult to deduce what logic operation is being performed at any one time. In other words, "gate-function-independence" as well as "data-independence" is achieved.

TABLE II. SIMULATION RESULTS COMPARING THE AVERAGE ENERGY DISSIPATION OF 2-INPUT GATES.

Frequency (MHz)	Logic Designs	AND/ NAND E_{av} (fJ)	OR/ NOR E_{av}(fJ	XOR/ XNOR E_{av} (fJ)	$E_{av,gate}$ (fJ)	σ (fJ)
1	[9]	5.740	4.275	3.328	4.617	1.214
	[10]	5.772	5.028	3.529	4.776	1.142
	proposed	5.869	5.868	5.870	5.869	0.001
10	[9]	6.053	5.116	3.908	5.025	1.075
	[10]	6.170	5.506	4.138	5.271	1.036
	Proposed	6.459	6.458	6.460	6.459	0.001
100	[9]	9.602	8.027	7.390	8.339	1.138
	[10]	9.787	8.648	8.027	8.820	0.892
	Proposed	10.690	10.69	10.691	10.69	0.001

C. Impact of Load Variations on Energy Dissipation

Shown in Fig. 5 is the influence of the load capacitance variation on the average energy consumption of AND/NAND gate using SPGAL, EE-SPFAL and the proposed logic at 10MHz at load capacitance of 10fF, 100fF, 200fF, and 300fF. As the proposed logic uses more number of transistors compared to SPGAL and EE-SPFAL, it has large internal load capacitance and therefore, dissipates more energy. However, the energy dissipation of the proposed logic approaches to that of SPGAL and EE-SPFAL at load capacitance higher than 100fF (Fig. 5). This is due to the fact that, at lower values of load capacitances, the load at the output nodes of the proposed logic will mostly be dominated by its internal load capacitance. In contrast, as the load capacitance value is increased, the effective load at the output nodes is dominated by the load capacitance rather than its internal load.

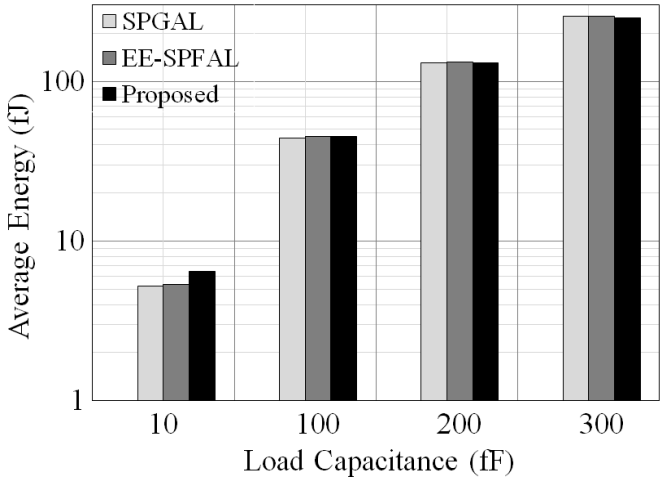


Fig. 5. Average Energy vs Load Capacitance for AND/NAND gate.

Case study: An 8-bit Montgomery Multiplier

To evaluate the performance of the proposed logic, an 8-bit Montgomery multiplier based on the radix-2 algorithm [13] was implemented. For comparison, SPGAL, and EE-SPFAL logic versions were also implemented.

A. Impact of Frequency Variations

Simulations for the Montgomery multiplier were performed at 1MHz, 13.56MHz and 100MHz frequencies. The energy dissipation was measured per cycle for 10 random input patterns. The simulation results are summarized in Table III. From Table III, proposed logic exhibits the least value of the %NED and %NSD for all the simulated frequencies followed by EE-SPFAL and SPGAL. Also, SPGAL failed to deliver the correct functionality at 1MHz due to the severe coupling effect which is caused by the absence of cross-coupled nMOS transistors. Because of the coupling effect, the output node which should remain at logic '0' gets coupled to the other output node following the power-clock. At low frequency (1MHz) the evaluating output node slowly follows the power-clock and therefore the coupled node gets enough time to follow the evaluating output node. As a result, the coupled output node reaches approximately 1.5V. This causes failure of functionality in SPGAL. At 13.56 MHz, due to the coupling effect, the coupled output node reaches almost 0.6V. At 100MHz, the coupled output node reaches nearly at 0.2V. This is the reason why 8-bit Montgomery multiplier using SPGAL dissipates more energy at 13.56 MHz in comparison to energy dissipated at 100MHz as can be seen from Table III.

TABLE III. COMPARING THE PERFORMANCE OF MONTGOMERY MULTIPLIER

Frequencies (MHz)	Logic Style	E_{av}(pJ)	%NED	%NSD
1	[9]	X	X	X
	[10]	3.154	5.684	2.416
	Proposed	5.232	0.122	0.060
13.56	[9]	5.217	14.00	7.768
	[10]	3.414	4.936	2.400
	Proposed	5.458	0.096	0.039
100	[9]	4.080	6.062	3.051
	[10]	4.117	3.610	1.878
	Proposed	6.981	0.190	0.091

B. Impact of Power-Clock Scaling on NED and NSD.

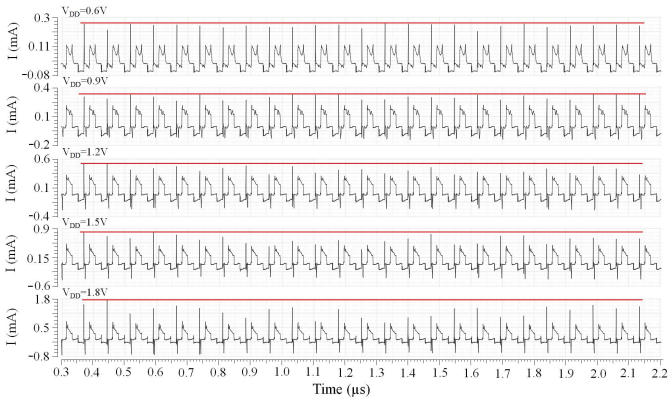
The supply voltage is one of the dominant components of the energy dissipation in adiabatic logic. Energy can be reduced if the power supply is reduced. Therefore, it is important to investigate how power-clock scaling influences the performance of the secure adiabatic logic design approaches.The power-clock was scaled from 1.8V down to 0.6V. The simulation results of the power-clock scaling at 13.56 MHz and 10fF load capacitance for 10 random inputs are summarized in Table IV. The simulation results for 1.8V power supply are omitted in Table IV because they were included in Table III. It can be seen that the proposed logic outperforms EE-SPFAL, and SPGAL at all power-clock values and exhibits the lowest value of %NED and %NSD. The performance of the EE-SPFAL is second best whereas, SPGAL performs worst at all power-clock values.

TABLE IV. COMPARING PERFORMANCE OF MONTGOMERY MULTIPLIER UNDER POWER SUPPLY SCALING

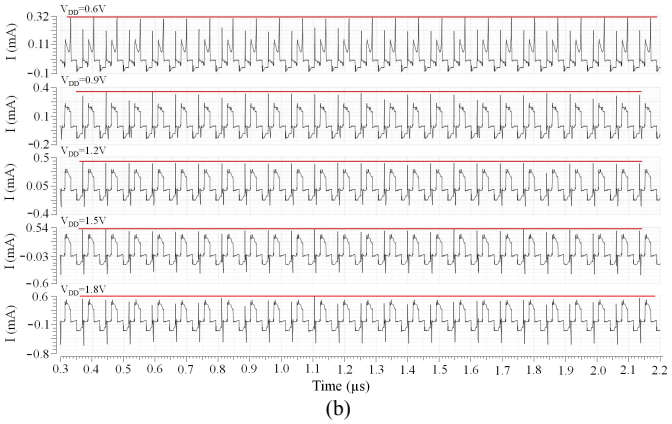
Logic Designs		Power-clock scaling @ 13.56MHz				
		V=0.6	*V=0.8*	*V=1.0*	*V=1.2*	*V=1.5*
[9]	E_{av}(pJ)	0.864	1.007	1.297	1.770	2.807
	%NED	1.303	3.449	4.260	5.531	8.625
	%NSD	0.586	1.490	1.737	2.505	4.447
[10]	E_{av}(pJ)	0.997	1.049	1.303	1.680	2.475
	%NED	0.689	1.819	2.976	3.612	4.182
	%NSD	0.293	0.883	1.177	1.693	1.535
Proposed	E_{av}(pJ)	1.568	1.746	2.131	2.723	3.953
	%NED	0.114	0.042	0.093	0.058	0.156
	%NSD	0.053	0.018	0.410	0.028	0.070

C. Impact of Power-Clock Scaling on Current Peaks.

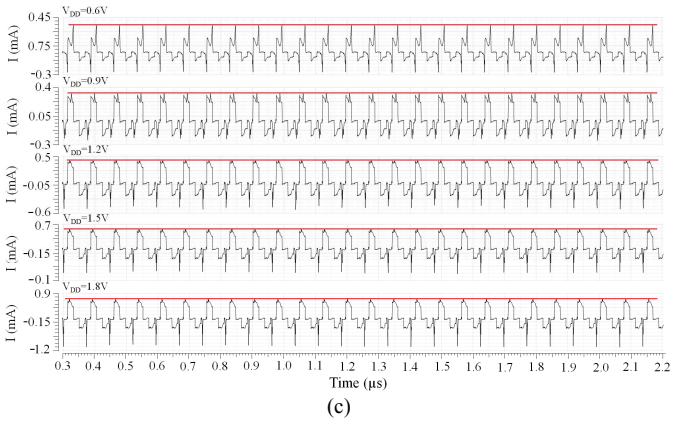
The current peaks for one complete computation of an 8-bit Montgomery multiplier using SPGAL, EE-SPFAL, and the proposed logic respectively are shown in Fig. 6 (a), (b), and (c).



(a)



(b)



(c)

Fig. 6. Current peaks for complete computation in 8-bit Montgomery multiplier at 13.56MHz using (a) SPGAL (b) EE-SPFAL and (c) Proposed

The current peaks are shown for a single set of input for power-clock phase 1 (PC1) ramping from 0V to $V_{DD,}$ where V_{DD} is scaled form 0.6V, to 1.8V at 13.56MHz. It can be seen that the 8-bit Montgomery multiplier implemented with the proposed logic exhibits the least variations in current peaks compared to the 8-bit Montgomery multiplier implemented with SPGAL and EE-SPFAL at all power-clock values. The 8-bit Montgomery multiplier using the proposed logic exhibits the variations of about 0.6% at 1.8V in the current peaks compared to the variations of 61.43%, and 14.66% for 8-bit Montgomery multiplier implemented with SPGAL and EE-SPFAL respectively. At 1.5V, the proposed logic exhibits the variations of 0.8% in the current peaks compared to the variations of approximately 46.52%, and 21.13% for the 8-bit Montgomery multiplier using SPGAL and EE-SPFAL respectively. At 1.2V, the proposed logic exhibits the variations of 1.45% whereas, the 8-bit Montgomery multiplier using SPGAL and EE-SPFAL exhibit the variations of 23.23%, and 41.88% respectively. At 0.9V, the proposed logic exhibits the variations of 1.22% whereas, the 8-bit Montgomery multiplier using SPGAL and EE-SPFAL exhibit the variations of approximately 17.23% and 24.85% respectively. Finally, at 0.6V, the proposed logic exhibits the variations of 2.35% whereas, the 8-bit Montgomery multiplier using SPGAL and EE-SPFAL exhibit the variations of approximately 23.07% and 4.23% respectively in the current peaks.

VI. Conclusion

This paper presented a new secure adiabatic logic approach using a single charge sharing transistor as a countermeasure against Power Analysis Attacks. The performance of the proposed logic was evaluated and compared with two existing secure adiabatic logic designs based on %NED, %NSD, current peak variations and energy dissipation. Simulations were performed and the impact of frequency variations and power-clock scaling on the %NED and %NSD was investigated and reported. Simulation results show that the proposed logic outperforms the existing logic designs and exhibits the least variations in current peaks and the lowest value of %NED and %NSD compared to the existing secure logic designs at all the simulated frequencies. Furthermore, 2-input gates using our proposed logic exhibit nearly the same average energy and the least value of standard deviation at all simulated frequencies. Therefore, "data-independence" as well as "gate-function independence" is achieved. The energy dissipation of the proposed logic reaches that of the two existing secure adiabatic logic designs for an output load capacitance over 100fF. The results exhibited by the gates were confirmed by using an 8-bit Montgomery multiplier as a design example for evaluation and comparison. Simulation results show that the proposed logic exhibits the least (i.e. best) value of %NED and %NSD under frequency variations and when the power supply was scaled from 1.8V down to .6V in comparison to the two existing logic designs.

Acknowledgment

The authors wish to thank University of Westminster for awarding Cavendish Research Scholarship for carrying out the research in the Department of Engineering.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, 1999, pp. 388-397.

[2] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan, "Investigations of power analysis attacks on smartcards", USENIX Workshop on Smartcard Technology Smartcard, 1999, pp.151–161.

[3] Thomas S Messerges, Ezzat A Dabbish, and Robert H Sloan. "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol. 51, no.5 , 2002, pp.541–552.

[4] C. Monteiro, Y. Takahashi, and T. Sekine, "DPA Resistance of charge sharing symmetric adiabatic logic," in Proc. of IEEE ISCAS'13, 2013, pp. 2581–2584.

[5] B.-D. Choi, K.E. Kim, K-S. Chung, and D.K. Kim, "Symmetric adiabatic logic circuits against differential power analysis," ETRI Journal, vol. 32, no. 1, 2010, pp. 166–168.

[6] M. Avital, H. Dagan, I. Levi, O. Keren, A. Fish, "DPA-Secure Quasi-Adiabatic Logic (SQAL) for Low-Power Passive RFID Tags Employing S-Boxes", IEEE Transactions on Circuits and Systems, vol. 62, no. 1, 2015, pp. 149 – 156.

[7] Y. Moon, and D.K. Jeong, "An efficient charge recovery logic circuit", in IEEE J. Solid-State Circuits, vol. 31, no. 4, 1996, pp. 514–522.

[8] A. Kramer, J.S. Denker, B. Flower, and J. Moroney, "2nd Order Adiabatic Computation 2N-2P and 2N-2N2P Logic Circuits", in Proceedings of the IEEE International Symposium on Low Power Design, 1995, pp.191–196.

[9] S. D. Kumar, H. Thapliyal, A. Mohammad, and S. K. Perumalla, "Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware," Integration, the VLSI Journal, vol. 58, 2016, pp. 369-377.

[10] S. Dinesh Kumar, H. Thapliyal, and A. Mohammad, "EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card," IEEE Transactions on Emerging Topics in Computing, vol. PP, no. 99, 2016, pp. 1-1

[11] A. Vetuli, S. Di Pascoli, and L. Reyneri, "Positive feedback in adiabatic logic," Electronics Letters, vol. 32, no. 20, 1996, pp. 1867–1868.

[12] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in Proc. ESSCIRC, Florence, Italy, 2002, pp. 403-406.

[13] A. Tenca and C. Koc, "A scalable architecture for modular multiplication based on Montgomery's algorithm,". IEEE Trans. on Computers, vol. 52, no. 9, 2003, pp. 1215–1221.