A Novel Power Analysis Attack Resilient Adiabatic Logic without Charge Sharing

Raghav, H., Bartlett, V. and Kale, I.

https://dx.doi.org/10.1109/ECCTD.2017.8093262

A Novel Power Analysis Attack Resilient Adiabatic Logic without Charge Sharing

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

***Abstract*— In this paper, we propose a novel power analysis attack resilient adiabatic logic which, unlike existing secure adiabatic logic designs doesn't require any charge sharing between the output nodes of the gates. The proposed logic also removes the non-adiabatic losses (NAL) during the evaluation phase of the power-clock. We investigate and compare our proposed and the existing secure adiabatic logic across a range of "power-clock" frequencies on the basis of percentage Normalized Energy Deviation (%NED), percentage Normalized Standard Deviation(%NSD) and average energy dissipation. The pre-layout and post-layout simulation results show that our proposed logic exhibits the least value of %NED and %NSD in comparison to the existing secure adiabatic logic designs at the frequency ranging from 1MHz to 100MHz. Also, our proposed logic consumes the lowest energy.**

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

I. INTRODUCTION

The Power Analysis Attacks (PAA) [1] attacks have received the most attention in recent years. In PAA, the adversary attempts to reveal secret information such as secret key, on the basis of the cryptographic device's power consumption during the execution of the critical operations such as encryption and decryption. The strength of the PAA comes from the fact that the power consumption of the cryptographic device depends on the intermediate values processed in it. Therefore, if the power consumption of the cryptographic device can be made independent of the intermediate values, the PAA can be made difficult. There are various countermeasures that have been proposed in the literature [2]-[10] to protect cryptographic implementations and are employed at the algorithmic level, architecture level, and cell (gate) level. Hiding [2] and masking [3] are amongst the most common countermeasures at cell level.

There are several papers that have addressed the design of PAA resilient logic designs such as Sense-Amplifier-Based Logic, SABL [2], Wave Dynamic Differential Logic, WDDL [4], Masked Dual-rail Pre-charge Logic (MDPL) [5], Three-phase Dual-rail pre-charged logic (TDPL) [6]. All these logic designs applied conventional CMOS logic operation and thus dissipate high energy.

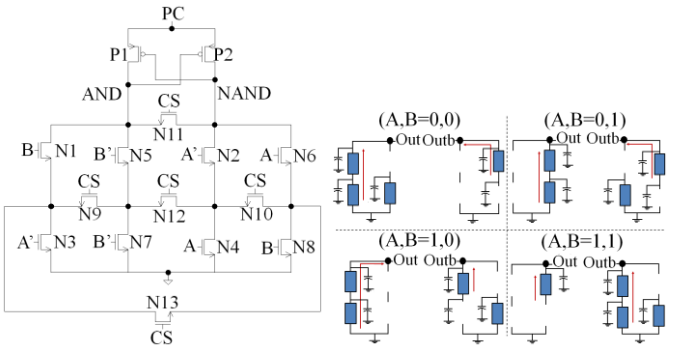
On the other hand, there are several, energy efficient PAA resilient logic designs based on the adiabatic logic [7] such as Charge-Sharing Symmetric Adiabatic logic, CSSAL [8]. Symmetric Adiabatic Logic, SyAL [9], and Secure Quasi-Adiabatic Logic, SQAL [10]. SyAL and SQAL are based on Efficient Charge Recovery Logic, ECRL [11]. SyAL and SQAL differ only in the number of charge-sharing transistors used. CSSAL on the other hand, is based on 2N-2N2P adiabatic logic [12] and is an enhancement of SyAL adiabatic logic. These existing adiabatic logic designs suffer from several shortcomings which will be discussed in section II. Section III, proposes, a novel PAA resilient adiabatic logic. Next, simulation results are presented in section IV where we investigate and compare our proposed and the existing secure adiabatic across a range of "power-clock" frequencies on the basis of % NED, % NSD, average energy dissipation. Also, a GF (2^4) bit-parallel multiplier design is presented as a design example to evaluate and compare the performance of the proposed and the existing adiabatic logic. Finally, a conclusion is formulated.

II. SHORTCOMINGS IN THE EXISTING SECURE ADIABATIC LOGIC DESIGNS

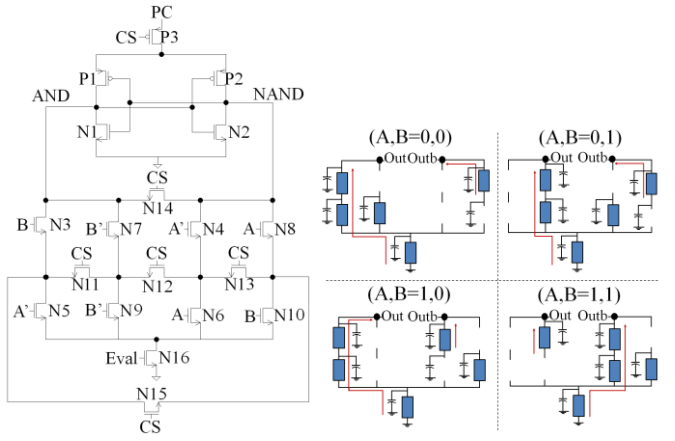
The existing PAA resistant logic has number of shortcomings. Firstly, all the logic designs use charge-sharing technique at the output/internal nodes of the gate to avoid dependency on the previous input transition. Apart from charge sharing, CS, inputs, CSSAL also uses an evaluation input. For working in cascade logic, the existing logic designs require 4-phase power-clocking scheme thus, incurs the overhead of generation, scheduling and routing of the 4-phases of the CS and evaluation input. Our proposed logic requires no additional inputs and thus saves this overhead.

Secondly, the existing logic designs suffer from Non-Adiabatic Losses (NAL) both in evaluation and recovery phase of the power-clock. Because the proposed logic uses dual evaluation network one connected between the power-clock and the output nodes and another connected between the output nodes and the ground thus, completely removes the NAL in the evaluation phase of the power-clock.

Thirdly, the existing logic gates are asymmetric. Fig. 1 (a), and (b) shows the AND/NAND gates and their equivalent RC models of the internal nodes during the evaluation phase for SyAL and CSSAL respectively. It can be observed that there is asymmetry in the gates. In none of the 4 input combinations, the same value of capacitance is charged at the two output nodes. The proposed logic charge the same capacitance value for each input combination.



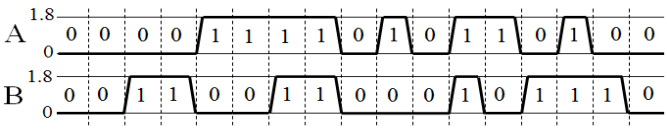
(a)



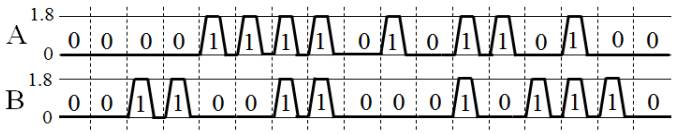
(b)

Fig. 1. Equivalent RC models of (a) SyAL AND/NAND [9] (b) CSSAL AND/NAND[8] gate during evaluation phase for 4 input combinations.

Lastly, the existing logic designs have been assessed for their resistance against PAA using the inputs which do not follow the adiabatic principle [8]. Also the inputs used are the one which will not come out of an adiabatic circuit. Fig. 2 (a) and (b) shows the 16 input transitions for 2-input gate as shown in [8] and the real life relevant adiabatic input transitions respectively. The problem with the input transitions of Fig 2(a) is that it favours the energy efficiency of the logic by removing the coupling effects and the NAL during the recovery phase of the power-clock. Simulation results show that there is an improvement of about 11%, 12.5%, 13.5% and 37% in the average energy dissipation of AND/NAND gate using CSSAL, SAQL, SyAL and the proposed logic respectively at 10MHz. There is a large improvement of average energy dissipation for the proposed logic because the input stays 'high' and stable even during the recovery phase of the power-clock thus, allows the full recovery of charge from the power-clock. This results in removal of NAL during the recovery phase.



(a)

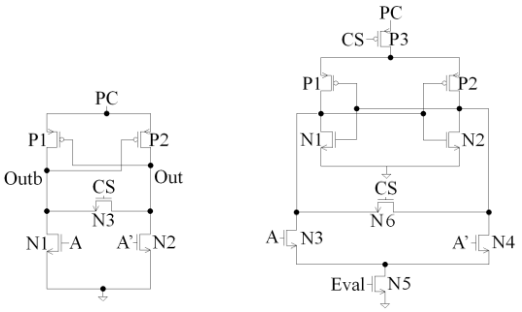


(b)

Fig. 2. 16 input transitions for 2-input gates (a) as given in [8] (b) real life relevent adiabatic input transistions.

III. Proposed Power Analysis Attack Resilient Adiabatic Logic Without Charge-Sharing

The idea of charge-sharing is to prepare the circuit for the evaluation of the next inputs by removing the remaining charge (due to non-adiabatic loss of the quasi-adiabatic logic) from the output nodes to avoid the data dependent initial condition which depends on the previous inputs. For removing the left over charge, charge-sharing transistors are used during the idle phase of the power-clock, before the evaluation of the next input take place. The NOT/BUF gate for SQAL and SyAL has the same structure and is shown in Fig 3(a). During the idle phase of the power-clock, when input A is rising transistor, N1 turns ON, and drives the output node 'Outb' to zero. As the charge-sharing transistor, N3, is also turned ON, it connects the output node, 'Out' to ground through transistor, N1. This way, both the output nodes are discharged to ground before the evaluation of the next inputs. The CSSAL NOT/BUF gate shown in Fig. 3 (b) uses an additional evaluation input apart from the charge-sharing transistors. The evaluation signal increases simultaneously with the input signal. The capacitances at the two output nodes are discharged to the ground before the logic function is evaluated.



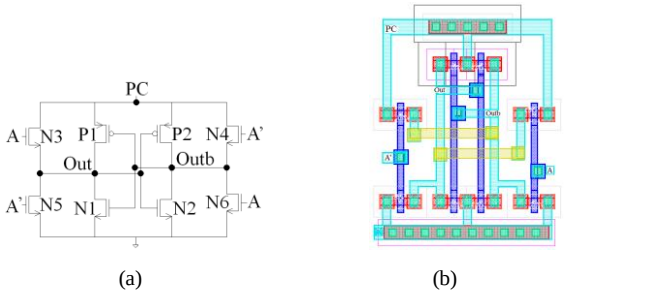
(a) (b)

Fig. 3. (a) SyAL/SQAL NOT/BUF [9],[10] schematic (b) CSSAL NOT/BUF [8] schematic.

We have proposed a novel PAA resilient adiabatic logic which does not require any charge-sharing between output nodes of the gates for discharging the output nodes to ground. Fig. 4(a) shows a NOT/BUF gate using the proposed logic. It uses dual evaluation network which helps both the output nodes to discharge to ground during the idle phase of the power-clock. It can be observed that during the idle phase of the power-clock when input A is rising transistors N3 and N6 are turned ON. Because the power-clock is at zero voltage during the idle phase, the output node 'Out' follows the power-

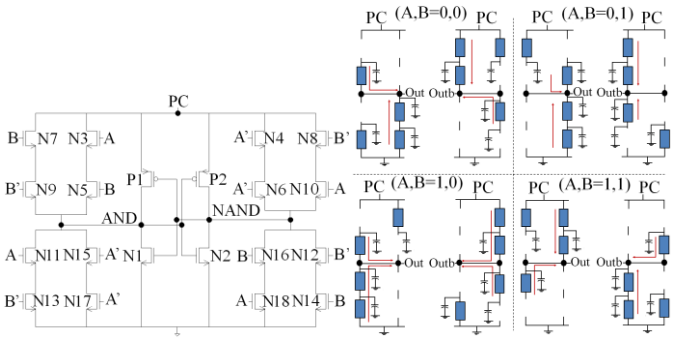
clock and makes it zero. Similarly, transistor N6 causes the output node 'Outb' to discharge to zero and thus no charge sharing is required. Fig. 4 (b) shows the layout for the NOT/BUF gate.

Fig. 5(a) and (b) shows the schematic and the equivalent RC models of the internal nodes of the proposed AND/NAND gate for 4 input combinations during the evaluation phase. It can be seen that for each input combination the same capacitance value is charged. The schematics of the OR/NOR, XOR/XNOR gates using proposed logic, were implemented in the similar way as the AND/NAND gate.



(a) (b)

Fig. 4. Proposed power analysis attack resilient NOT/BUF gate (a) Schematic (b) Layout.



(a) (b)

Fig. 5. Proposed power analysis attack resilient AND/NAND gate (a) Schematic (b) Equivalent RC model in evaluation phase.

IV. Simulation Results

Simulations were performed in 'typical-typical' process corner using TSMC 180nm CMOS process at 1.8V power supply. The load capacitance was chosen as 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 pre-layout simulations were performed at frequencies 1MHz, 10MHz and 100MHz and the energy dissipation per cycle for all possible input transitions for NOT/BUF and 2-input gates were measured for existing and the proposed logic.

The pre-layout simulation results are summarised in Table I. To quantify the resistance of the proposed and the existing logic designs, we measured the maximum energy value (E_{max}), minimum energy value (E_{min}), the average energy value (E_{av}), and the standard deviation (σ) for all the possible input transitions for NOT/BUF and 2-input gates. From these values, we obtained the Normalised Energy Deviation (NED) and Normalised Standard Deviation (NSD), according to (1) and (2).

The Normalised Energy Deviation (NED) is defined as:

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

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

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

Where, E_{av} is the average energy dissipation for all 16 input transitions, and Standard Deviation is defined as:

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

Table I shows that the proposed logic exhibits the least value of %NED and %NSD at all simulated frequencies. It also shows that at 1MHz, the energy consumption of the 2-input gates using proposed logic is greater than SQAL and SyAL and is comparable to CSSAL. However, SQAL, SyAL and CSSAL suffers from NAL during the evaluation and recovery phase of the power-clock whereas, the proposed logic suffers from NAL only during the recovery phase.

At low frequencies, the energy dissipation of the adiabatic logic in general is dominated by leakage energy rather than Adiabatic Losses (AL) and NAL. Thus, the proposed logic having more transistors than SQAL and SyAL dissipates more energy. CSSAL on the other hand, has 19 transistors and has higher NAL thus, consumes more energy than the proposed logic. Also, NAL of CSSAL is higher compared to SQAL and SyAL, because it has 2 stacked transistors, one connected between the input and the ground and the other connected between the power-clock and the cross-coupled pMOS transistors P1 and P2 as shown in Fig. 3 (b).

AL dominates at higher frequencies rather than leakage loss. Thus, at 10 MHz and 100 MHz AL combined with NAL leads to large energy dissipation in CSSAL, SQAL and SyAL compared to the proposed logic as can be seen from Table I. It also shows that on the basis of %NED and %NSD, the performance of SQAL, SyAL and CSSAL changes with frequency. At 1MHz and 100MHz, CSSAL is second best followed by SyAL and SQAL, whereas, at 10 MHz, SyAL is second best and is followed by CSSAL and SQAL. Thus, the ranking of performance (security level) of the existing logic is frequency dependent. The proposed logic outperforms the existing secure adiabatic logic at all simulated frequencies.

Galois field *(GF)* arithmetic plays an important role in cryptography algorithms. To evaluate the performance of the proposed logic a *GF* (2^4) bit-parallel multiplier was implemented. For comparison, CSSAL, SQAL and SyAL versions were also implemented. The simulations were performed under the same conditions as for the gates. The % NED and % NSD were calculated for 15 random inputs at all simulated frequencies.

TABLE I.PRE-LAYOUT SIMULATION RESULTS COMPARING THE %NED OF NOT/BUF AND 2-INPUT GATES USING CSSAL, SQAL, SYAL AND PROPOSED LOGIC.

Logic designs	CSSAL[8]			SQAL[10]			SyAL[9]			Proposed		
	1MHz	*10MHz*	*100MHz*	*1MHz*	*10MHz*	*100MHz*	*1MHz*	*10MHz*	*100MHz*	*1MHz*	*10MHz*	*100MHz*
NOTBUF												
Eav (fJ)	3.314	6.340	19.540	2.415	4.276	12.180	2.415	4.276	12.180	1.792	2.479	5.685
% NED	0.781	1.223	0.814	2.050	1.163	0.735	2.050	1.163	0.735	0.445	0.523	0.351
% NSD	0.453	0.710	0.377	0.920	0.675	0.358	0.920	0.675	0.358	0.257	0.281	0.176
AND/NAND												
Eav (fJ)	6.500	10.350	28.710	4.892	7.137	17.870	5.434	7.760	19.253	5.837	6.438	10.674
% NED	1.115	1.914	1.073	2.384	2.985	3.685	1.933	1.332	1.546	0.562	0.186	0.187
% NSD	0.458	0.599	0.456	1.169	1.033	1.505	0.810	0.409	0.619	0.167	0.047	0.076
OR/NOR												
Eav (fJ)	6.499	10.360	28.710	4.890	7.129	17.840	5.435	7.765	19.233	5.838	6.439	10.674
% NED	1.161	1.820	1.010	2.384	3.065	3.630	1.988	0.922	1.597	0.528	0.124	0.187
% NSD	0.483	0.596	0.442	1.169	1.109	1.444	0.813	0.330	0.610	0.165	0.034	0.076
XOR/XNOR												
Eav (fJ)	6.503	10.370	28.720	5.152	7.368	17.090	5.444	7.761	19.235	5.840	6.440	10.676
% NED	0.964	1.726	1.040	0.658	0.095	0.992	1.808	1.589	1.444	0.545	0.047	0.187
% NSD	0.477	0.474	0.428	0.179	0.032	0.318	0.573	0.385	0.592	0.183	0.019	0.068
$GF(2^4)$												
Eav (fJ)	181.63	230.34	531.98	159.32	167.79	272.74	175.96	196.56	371.6	175.46	184.59	242.75
% NED	1.824	2.520	2.026	3.180	1.926	1.870	2.895	2.770	1.608	0.935	0.824	0.783
% NSD	0.655	0.795	0.625	1.494	0.827	0.817	1.515	1.209	0.686	0.456	0.523	0.365

Table I shows that the *GF* (2^4) multiplier results confirms those repetition from the pre-layout and post-layout simulation results of the gates.

The full-custom layouts were drawn using Cadence Virtuoso™ layout editor. The post-layout simulations were carried out for each of the existing and proposed logic designs. The layouts for all the gates were drawn keeping the symmetry and output node load balancing in mind. The post-layout simulation results shows the similar trend as shown by the schematics except that the %NED and %NSD are large for each of the proposed and the existing designs compared to their corresponding %NED and %NSD in pre-layout simulation results. The proposed logic outperforms the existing secure adiabatic logic at all simulated frequencies.

V. CONCLUSION

In this paper, we have proposed a novel power analysis attack resilient adiabatic logic which does not require any charge-sharing between the output nodes of the gate. The proposed logic completely removes the non-adiabatic losses during the evaluation phase of the power-clock. The full-custom layouts were drawn for the proposed and the existing adiabatic logic. The pre-layout and post-layout simulation results show that our proposed logic shows less variation in % NED and % NSD with frequency variations compared to existing adiabatic logic. Also our proposed logic exhibits the least value of the % NED and % NSD at all simulated frequencies. These results were confirmed by using *GF* (2^4) bit-parallel multiplier as a candidate circuit for comparison.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. Advances in Cryptography, pp. 388-397, 1999.

[2] 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. 28th European Solid-State Circuits Con/. (ESSCIRC '02), pp. 403-406, 2002.

[3] J. D. Golic and R. Menicocci, "Universal Masking on Logic Gate Level", Electronics Lett., vol. 40, no. 9, pp. 526-528, 2004.

[4] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," In Design, Automation and Test in Europe Conference and Exposition, pp. 246-251, 2004.

[5] T. Popp and S. Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints", Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '05), Lecture Notes in Computer Science, vol. 3659, pp. 172-186, 2005.

[6] M. Bucci, L. Giancane, R.o Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Precharge Logic," In Cryptographic Hardware and Embedded Systems – CHES 2006, LCNS, vol. 4249, pp. 232-241, 2006.

[7] W. C. Athas, L. J. Svesson, J. G. Koller, N. Traztzanis and E. Y.-C. Chuo, "Low power digital system based on adiabatic-switching principles,"IEEE Trans. VLSI Syst. , vol. 2, no. 4, pp. 398-406, 1994.

[8] C.Monteiro,Y.Takahashi,T.Sekine, "Resistance against power analysis attacks on adiabatic dynamic and adiabatic differential logic designs for smartcard", Proceedings of the IEEE Intelligent Signal Processing and Communication System (ISPACS'11), pp.1–5, 2011.

[9] 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, pp. 166–168, 2010.

[10] 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, pp. 149 – 156, 2015.

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

[12] 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, pp.191–196, 1995.