Robustness of Power Analysis Attack Resilient Adiabatic Logic: WCS-QuAL under PVT Variations

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

This is a copy of the author's accepted version of a paper subsequently published in the proceedings of the *27th International Symposium on Power and Timing Modeling, Optimization and Simulation,* Thessaloniki, Greece, 25 to 27 Sep 2017, IEEE.

It is available online at:

https://dx.doi.org/10.1109/PATMOS.2017.8106968

Robustness of Novel Power Analysis Attack Resilient Adiabatic Logic against PVT Variations

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 Without Charge Sharing Quasi Adiabatic Logic (WCS-QuAL) as a countermeasure against Power Analysis Attacks. We evaluate and compare our logic with the recently proposed secure adiabatic logic designs SPGAL and EE-SPFAL at frequencies ranging from 1MHz to 100MHz. Simulation results show that WCS-QuAL outperforms the existing secure adiabatic logic designs on the basis of %NED and %NSD at all simulated frequencies. Also, all three 2-input gates using WCS-QuAL exhibits logic operation independent energy dissipation by dissipating nearly equal energy. Also, the energy dissipated by WCS-QuAL approaches to the energy dissipation of EE-SPFAL and SPGAL as the output load capacitance is increased above 100fF. To further evaluate and compare the performance GF (2^4) bit-parallel multiplier was implemented as a design example. The impact of PVT variations, power supply scaling and technology on the performance of the three logic designs was investigated and compared. Simulation results show that WCS-QuAL passed the functionality test against PVT variations and can perform well against the power supply scaling (from 1.8V to 0.5V). It also exhibits the least value of %NED and %NSD against PVT variations and when the power supply is scaled from 1.8V to 0.5V compared to EE-SPFAL and SPGAL. Also, the difference in energy dissipation between WCS-QuAL and EE-SPFAL decreases at tsmc 90nm technology.**

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

I. INTRODUCTION

Power Analysis Attacks (PAA) are considered to be the most powerful attacks as they are based on the monitoring of the power supply currents during the execution of critical operations such as encryption/decryption. By this, an attacker can deduce the secret key used in the cryptographic device. PAA such as Differential Power Analysis attacks (DPA) [1-2] uses statistical methods and digital processing techniques on a large number of monitored power signals. Such methods reduce noise and enhance the signal making it easier to distinguish between zero and one.

PAA can be resisted if the power consumption of the device can be made independent of input data being processed in the cryptographic device. Countermeasures at the cell/gate level require building the cryptographic device using gates that are resilient to PAA. The power consumption of the cryptographic device is the total of the power consumed by its gates. Therefore, if the power consumption of the gates is made independent of the input data processed, the cryptographic device can be made resilient to PAA.

Hiding [3] and masking [4] are amongst the most common countermeasures used at the cell/gate level. In hiding, the cryptographic device's power consumption characteristics are changed in a way that every operation consumes nearly same energy. Dynamic and differential logic styles are used to make the power consumption of the device independent of the input data. Unlike hiding, masking relies on randomizing the input/key dependent intermediate values processed during the execution of the cryptographic device. With this method, the power consumption of the cryptographic device is randomized thus, making it largely 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 shortcomings of the existing logic designs are discussed in section III. The proposed logic, WCS-QuAL is presented in section IV. In section V, simulation results are presented. Finally, the paper is concluded in section VI.

II. BACKGROUND

There are numerous papers that have addressed the design of PAA resistant logic such as Masked Dual-rail Pre-charge Logic (MDPL) [7], Dual-rail Random Switching Logic (DRSL) [8], Sense-Amplifier-Based Logic (SABL) [5], Wave Dynamic Differential Logic (WDDL) [6], Three-phase Dual-rail pre-charged logic (TDPL) [9]. All these countermeasures applied conventional CMOS logic operation and thus are not energy efficient.

There are several energy efficient PAA resistant logic designs which are based on the adiabatic logic [10]-[17] such as Charge-Sharing Symmetric Adiabatic Logic (CSSAL) [10], Symmetric Adiabatic Logic (SyAL) [11], and Secure Quasi-Adiabatic Logic (SQAL) [12]. All of these design styles make use of charge-sharing technique at the output/internal nodes and load balancing at the two output nodes to guarantee constant energy consumption. SyAL and SQAL are based on Efficient Charge Recovery Logic (ECRL) [13]. The difference between SyAL [11] and SQAL [12] is in the number of charge-sharing transistors used. Alternatively, CSSAL is based on 2N-2N2P adiabatic logic [14] and is an enhancement of SyAL adiabatic logic. CSSAL consumes more energy, has a complex structure (using two additional inputs in the gate). SyAL, SQAL and CSSAL use pull down evaluation network and thus

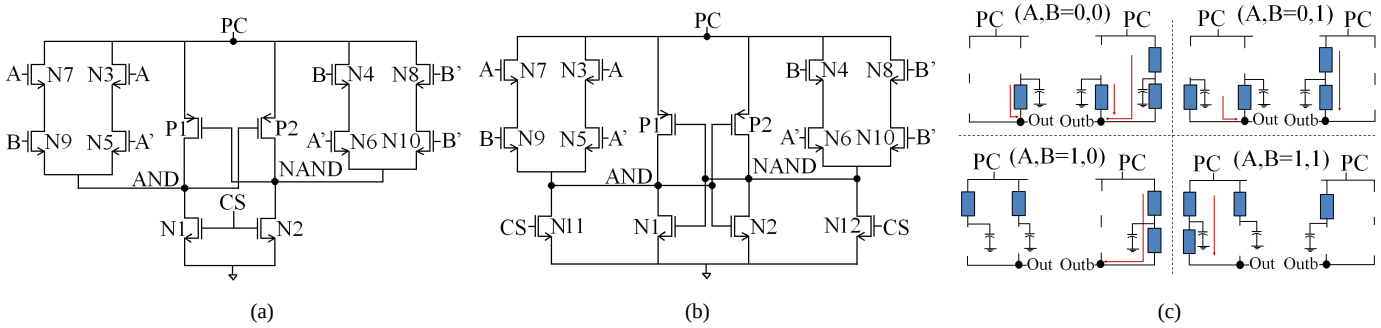

Fig. 1. AND/NAND gates (a) SPGAL[15], [16] (b) EE-SPFAL [17](c) Equivalent RC model of SPGAL/EE-SPFAL.

suffer from Non-Adiabatic Losses (NAL) during the evaluation phase of the power-clock and dissipate more energy. Because they use additional inputs thus, present the overhead of generation, scheduling, and routing of additional input, charge-sharing.

Symmetric Pass Gate Adiabatic Logic (SPGAL) [15], [16] and Energy Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) [17] are the secure adiabatic logic design styles which do not suffer from NAL during the evaluation phase of the power-clock. However, both of these logic designs require an additional discharge input in order to discharge the two output nodes before the evaluation of the next inputs. Thus, incur the overhead of generation, scheduling, and routing of the discharge signal.

Since our proposed logic, Without Charge Sharing Quasi Adiabatic Logic (WCS-QuAL) also doesn't suffer from non-adiabatic losses during the evaluation phase of the power-clock. Also, SPGAL [15], [16] and EE-SPFAL [17] are the recently proposed secure adiabatic logic designs, and have proven to be better than CSSAL [10], SyAL [10] and SQAL [10], a comparison of the performance between WCS-QuAL, SPGAL and EE-SPFAL on the basis of %NED and %NSD and energy dissipation is presented in this paper. To further evaluate and compare the performances, Galois Field, GF (2^4) bit-parallel multiplier was implemented and the impact of Process, Voltage, and Temperature (PVT) variations, power supply scaling and technology was investigated.

III. Shortcomings in the Existing Logic Designs

SPGAL[15], [16] and EE-SPFAL[17] secure adiabatic logic designs suffer from several shortcomings:

Firstly, SPGAL[15], [16] and EE-SPFAL[17] require additional input called discharge/charge sharing input at the output nodes to discharge the left over charge before the next inputs are evaluated. This input is active only during the idle phase of the power-clock. Since both EE-SPFAL and SPGAL are based on Positive Feedback Adiabatic Logic (PFAL)[18] thus require 4 phase power-clocking scheme to work in cascade logic. Therefore, in a system design using EE-SPFAL and SPGAL, four phases of the charge sharing inputs are required thus incurring the overhead of generation, scheduling, and routing of the signal. This will also add to additional energy dissipation. Since WCS-QuAL doesn't require any additional input thus, saves this overhead.

Secondly, they are asymmetric. Fig. 1 (a), (b) and (c) shows the schematic of the AND/NAND gate using SPGAL, EE-SPFAL and its 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 PFAL [18]. From Fig. 1 (c), it can be seen that for none of the input combinations, the two output nodes charge the same value of capacitance. This difference in capacitance value brings the difference in energy dissipated for different input transitions. However, WCS-QuAL charge the same capacitance for each input combination (shown in Fig. 4(b)).

Thirdly, the structure of SPGAL is unstable due to the absence of cross-coupled pull down network as can be seen from Fig. 1(a). When one of the output nodes follow the power-clock, the complementary node gets coupled to it during evaluation, hold, and recovery phase of the power-clock. This result in the complimentary node voltage to rise above the threshold voltage (V_{tn}) thus dissipates more energy.

Lastly, SPGAL has a greater chance of failing to deliver correct functionality at power supply close to V_{tn}. From Fig. 2 (a), it can be seen that the nMOS evaluation transistors (N3 and N4) connected between the power-clock and the output nodes will fail to raise the output above V_{DD}-V_{tn}. At this point, the pMOS transistors (P1 or P2) helps in charging the output node to V_{DD} but due to the absence of cross-coupled nMOS transistors, one of the output nodes which should remain at zero gets coupled to the node following the power-clock. This leads to wrong functionality at power supply close to V_{tn}. Due to dual evaluation network in WCS-QuAL, it can work at a supply voltage as low as V_{tn}.

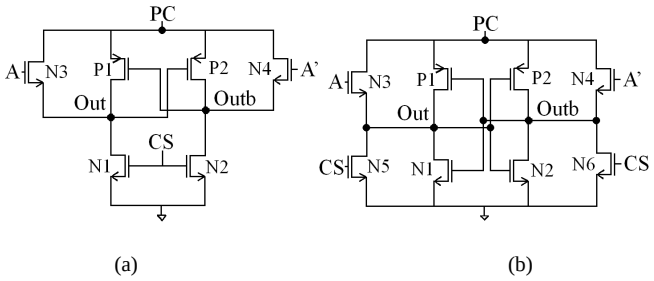

Fig. 2. NOT/BUF gate using (a) SPGAL [15], [16] (b) EE-SPFAL [17].

IV. Proposed Logic Without Charge Sharing

Charge sharing/discharging is done to remove the remaining charge from the output nodes of the circuit before the evaluation of the next inputs. This is required to escape the data dependent initial condition which has a dependency on the previous inputs. Charge sharing/discharge transistors are active only during the idle phase of the power-clock (PC).

WCS-QuAL does not require any charge sharing between the output nodes of the gates to discharge the output nodes to ground. Fig. 3(a) and (b) shows a NOT/BUF gate using WCS-QuAL and the timing diagram respectively for 4 input transitions. The operation is explained for input, A=1 and A'=0 From Fig. 3(b) it can be observed that during the Idle phase (I) of the power-clock when input A is rising, transistors N3 and N6 (Fig. 3(a)) are turned ON when the gate voltage is greater than the threshold voltage (V_{tn}). Because the power-clock is low (zero) during the idle phase, the source node 'Out' of transistor N3 will also be at zero, and there will not be any current flow through N3. Similarly, the transistor, N6 causes the output node 'Outb' to discharge to ground (charge left of the previous cycle). Thus the two output nodes are discharged to zero before the Evaluation phase (E) of the power-clock begins. Hence, no discharging input transistors are required.

During the Evaluation phase (E), input A is already at V_{DD} and the power-clock starts rising from zero to 1.8V. Like SPGAL and EE-SPFAL, the proposed WCS-QuAL also has reduced ON-resistance, due to the formation of transmission pair (N3, P1) and eliminates the Non-Adiabatic Loss (NAL).

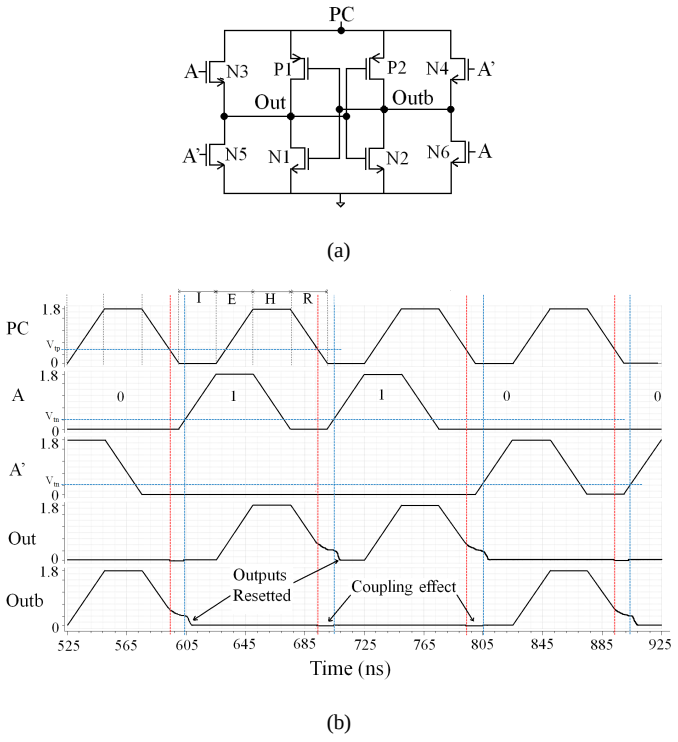

Fig. 3. (a) WCS-QuAL NOT/BUF gate (b) Timing Diagram

During the Hold phase (H), the power-clock is at 1.8V and the input A is falling from 1.8V to zero. When the gate-to-source voltage of transistor, N3 falls below Vtn, transistor N3 will be switched off and the output nodes 'Out' and 'Outb' are held at their respective voltage due to the cross-coupled transistors (P1, P2, and N1, N2).

During the Recovery phase (R), the power-clock ramps down from 1.8V to zero. The charge stored on the 'Out' node is recovered back to the power-clock through the transistor, P1. The recovery of the charge continues until P1 reaches its threshold voltage, $|V_{tp}|$. At this time, P1 is turned off and the output node 'Out' stays at V_{tp}. It will only be discharged to ground, in the idle phase of the power-clock when the next input arrives and its gate voltage is greater than the threshold voltage (V_{tn}) as shown in Fig. 3 (b). The output nodes are floating when the power-clock reaches it threshold voltage until one of the evaluation transistors are turned ON, thus the complementary node 'Outb' goes below zero voltage due to the coupling effect. Thus, WCS-QuAL suffers from coupling effect for small duration. Since SPGAL does not have cross-coupled nMOS transistors (N1 and N2) the nodes remain floating for the whole period of the recovery phase.

Fig. 4 (a) and (b) shows the schematic of the WCS-QuAL AND/NAND gate and the equivalent RC model of the internal nodes during the evaluation phase for 4 input combinations. It can be seen that the two output nodes are balanced for each input combinations. All 2-input gates using proposed logic have the same structure.

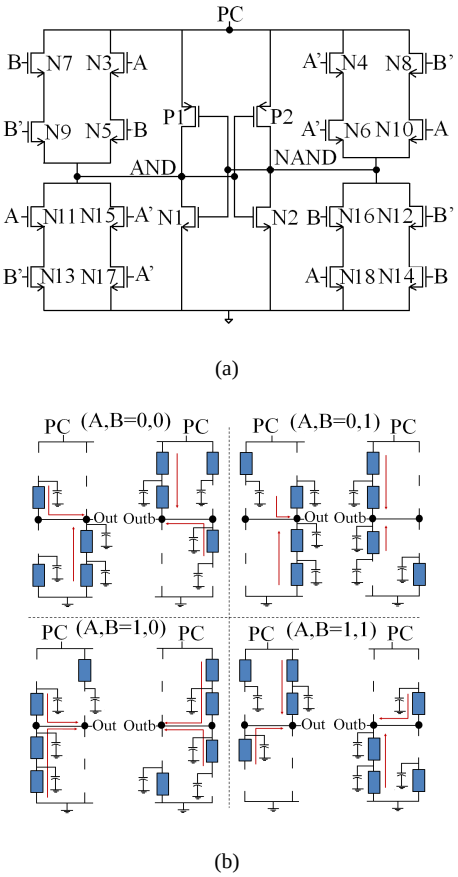

Fig. 4. WCS-QuAL (a) AND/NAND gate (b) Equivalent RC models.

V. SIMULATION RESULTS

Simulations for all the secure adiabatic logic designs were performed with Spectre simulator using Cadence EDA tool in a 'typical-typical', TT process corner using TSMC 180nm CMOS process at 1.8V power supply. The load capacitance chosen was 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 performed at 1MHz, 10MHz and 100MHz frequencies. The energy dissipation per cycle was measured for all possible input transitions for NOT/BUF and 2-input gates for WCS-QuAL, SPGAL, and EE-SPFAL.

To evaluate the resistance of WCS-QuAL, SPGAL, and EE-SPFAL against PAA, we obtained the Normalised Energy Deviation (NED) and Normalised Standard Deviation (NSD), 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 value of %NED and %NSD and lower the cell's vulnerability to power analysis attacks.

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 WCS-QuAL, SPGAL and EE-SPFAL are summarised in Table I. It can be seen that on the basis of %NED and %NSD, the performance of WCS-QuAL is the best as it exhibits the least value of %NED and %NSD followed by EE-SPFAL and SPGAL at 1MHz, 10MHz, and 100MHz.

Table I also shows that the energy dissipation of WCS-QuAL for 2-input gates is greater than SPGAL and EE-SPFAL at all simulated frequencies. At 1 MHz, WCS-QuAL dissipates approximately 25% and 21% more energy compared to SPGAL and EE-SPFAL respectively. At 100MHz, WCS-QuAL dissipates nearly 23% and 16% more energy in comparison to SPGAL and EE-SPFAL respectively. At 100MHz, the energy dissipated by WCS-QuAL decreases in comparison to the energy dissipated at 1MHz.

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		
	SPGAL [15], [16]	**EE-SPFAL [17]**	**WCS-QuAL**	**SPGAL [15], [16]**	**EE-SPFAL [17]**	**WCS-QuAL**	**SPGAL [15],[16]**	**EE-SPFAL[17]**	**WCS-QuAL**
NOT/BUF									
E_{max} (fJ)	1.770	1.796	1.796	2.390	2.461	2.486	5.387	5.736	5.700
E_{min} (fJ)	1.736	1.787	1.788	2.385	2.451	2.473	5.343	5.713	5.680
E_{av} (fJ)	1.755	1.792	1.792	2.387	2.455	2.479	5.352	5.725	5.685
σ(fJ)	0.012	0.004	0.004	0.002	0.003	0.007	0.019	0.009	0.010
%NED	1.920	0.501	0.445	0.209	0.406	0.523	0.816	0.400	0.351
%NSD	0.725	0.255	0.257	0.114	0.147	0.281	0.365	0.174	0.176
AND/NAND									
E_{max} (fJ)	5.816	5.861	5.862	6.286	6.075	6.442	9.684	10.100	10.680
E_{min} (fJ)	5.246	5.465	5.829	5.801	5.771	6.430	8.941	9.477	10.660
E_{av} (fJ)	5.740	5.772	5.837	6.253	6.009	6.438	9.602	9.787	10.674
σ(fJ)	0.135	0.132	0.009	0.120	0.106	0.008	0.177	0.309	0.008
%NED	9.800	6.756	0.562	7.715	5.004	0.186	7.672	6.168	0.187
%NSD	2.355	2.290	0.167	1.928	1.772	0.047	1.843	3.163	0.076
OR/NOR									
E_{max} (fJ)			5.861			6.442			10.680
E_{min} (fJ)			5.830			6.434			10.660
E_{av} (fJ)	X	X	5.838	X	X	6.439	X	X	10.674
σ(fJ)			0.009			0.002			0.008
%NED			0.528			0.124			0.187
%NSD			0.165			0.034			0.076
XOR/XNOR									
E_{max} (fJ)	3.355	3.538	5.861	3.912	4.141	6.642	7.410	8.034	10.680
E_{min} (fJ)	3.307	3.519	5.829	3.907	4.137	6.439	7.365	8.020	10.660
E_{av} (fJ)	3.328	3.529	5.840	3.908	4.138	6.440	7.390	8.027	10.676
σ(fJ)	0.010	0.005	0.010	0.002	0.001	0.001	0.010	0.004	0.007
%NED	1.430	0.537	0.545	0.127	0.096	0.047	0.607	0.174	0.187
%NSD	0.310	0.146	0.183	0.057	0.024	0.019	0.148	0.062	0.068

X denotes that OR/NOR gate circuits for SPGAL and EE-SPFAL are not available.

WCS-QuAL dissipates more energy as it has more transistors than SPGAL and EE-SPFAL. Also, WCS-QuAL uses dual evaluation network one connected between the output nodes and the power-clock and the other connected between the output nodes and ground thus have high internal node capacitance than SPGAL and EE-SPFAL. Therefore, at lower values of load capacitances, the load at the output nodes of WCS-QuAL will mainly be dominated by its internal load capacitance and thus dissipates more energy than SPGAL and EE-SPFAL.

B. Logic operation independent energy disspation.

Table II shows the average energy dissipated for all possible input transitions of AND/NAND, OR/NOR and XOR/XNOR gates using WCS-QuAL and AND/NAND and XOR/XNOR gates using SPGAL and EE-SPFAL. It also shows the standard deviation (σ) of average energy dissipated by AND/NAND, OR/NOR and XOR/XNOR at all the simulated frequencies. It can be seen that 2-input gates using WCS-QuAL dissipates approximately the same energy at all simulated frequencies. This will have an advantage in a complex circuit where it will be difficult to identify which logic operation is being executed. It can also be seen that WCS-QuAL shows the least value of standard deviation in comparison to SPGAL and EE-SPFAL.

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	SPGAL	5.740	X	3.328	4.534	1.705
	EE-SPFAL	5.772	X	3.529	4.650	1.586
	WCS-QuAL	5.837	5.838	5.838	5.838	0.001
10	SPGAL	6.253	X	3.908	5.080	1.658
	EE-SPFAL	6.009	X	4.138	5.073	1.323
	WCS-QuAL	6.438	6.439	6.440	6.439	0.001
100	SPGAL	9.602	X	7.390	8.496	1.564
	EE-SPFAL	9.787	X	8.027	8.907	1.245
	WCS-QuAL	10.674	10.674	10.676	10.67	0.001

X denotes that OR/NOR gate circuits for SPGAL and EE-SPFAL are not available.

C. Impact of load variations on energy dissipation.

Fig. 5 shows the effect of loading on average energy consumption of AND/NAND gate using WCS-QuAL, SPGAL, and EE-SPFAL at 10MHz. In comparison to SPGAL, both EE-SPFAL and WCS-QuAL has more internal node capacitance due to discharging transistors and dual evaluation network respectively. Thus at lower load capacitance values, their energy is almost same for 2 input AND/NAND gate. The difference in their energy dissipation is due to the fact that charge sharing transistors are turned ON for a ¼ period of the power-clock whereas; the dual evaluation network is turned ON for a ¾ period of the power-clock. Thus, WCS-QuAL dissipates more energy.

The structure of XOR/XNOR gate using WCS-QuAL is different from the structure using SPGAL and EE-SPFAL. WCS-QuAL uses eight transistors connected between power-clock and the output nodes whereas, EE-SPFAL and SPGAL use six transistors connected between power-clock and the output nodes. Thus WCS-QuAL dissipates more energy.

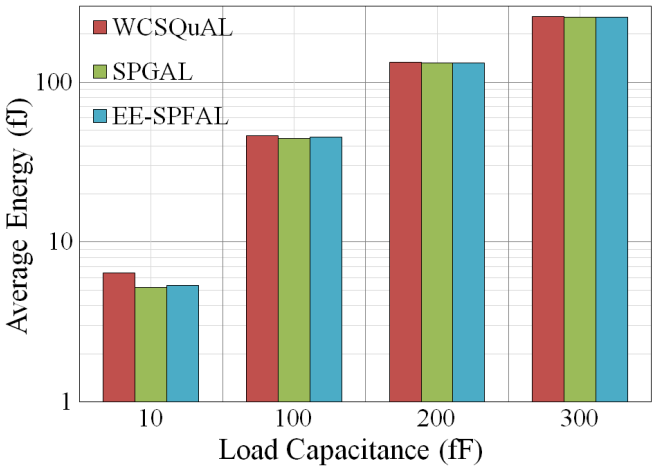

Fig. 5. Average Energy vs Load Capacitance for AND/NAND gate.

However, the energy dissipated by WCS-QuAL approaches approximately to energy dissipation of SPGAL and EE-SPFAL at load capacitance values higher than 100fF as can be seen from Fig. 5. This is because, at lower values of load capacitances, the load at the output nodes of WCS-QuAL will mainly be dominated by its internal load capacitance as it has more transistors. Contrary to this, as the load capacitance value is increased, the effective load at the output node will be dominated by the load capacitance rather than its internal load.

Case study: GF (2^4) bit parallel Multiplier

Galois Field or Finite field plays an important role in the field of modern cryptography. A GF (2^m) field is an extension of the GF (2), with elements {0, 1}. GF (2^4) bit-parallel Multiplier was chosen as the candidate circuit to evaluate and compare the performance of WCS-QuAL, SPGAL, and EE-SPFAL logic.

A. Impact of Process, Temperature and Voltage Variations.

A countermeasure that can be confirmed secure at a high abstraction level is not necessarily secure when supply voltage scaling, load capacitances, process variations, frequency of operation are taken into account [19]. Thus, it is important to perform the simulation-based evaluations exhaustively by creating an environment which depicts the physical reality. Process variations impact the data-dependence of both dynamic and leakage power. Process and environmental variations are an additional factor that can deteriorate the resistance against PAA of the secure logic designs. In adiabatic logic, process variations have an impact on the circuit performance specifically, on energy dissipation. Process variations induce changes in threshold voltage and thus shift in the optimum frequency[20]. Therefore, it is

important to evaluate the robustness of the secure adiabatic logic designs against PVT variations.

To measure the robustness of the three adiabatic logic designs against PVT variations, we considered the corner analysis to check the functionality and resistance against PAA at worst and the best case conditions. The temperature and voltage values, for the even corners Fast-Fast 'FF' and Slow-Slow 'SS' were chosen in order to get the worst and best case energy dissipation. The worst case energy dissipation was calculated for FF process corner at 1.98V supply voltage and 100^0C temperature. This is because; the energy dissipation has a quadratic dependence on V_{DD} whereas, increased temperature increases the on-resistance of the charging path[20]. Similarly, for the best case scenario, 1.62V supply voltage, and 0^0C temperature were chosen.

For the skewed corners 'SF' and 'FS', designs were simulated for all 4 combinations of temperature and supply voltage and the skewed values of the temperature and voltage corresponding to fast nMOS and slow pMOS or vice-versa were chosen. For 'SF' corner the supply voltage and temperature were chosen as 1.62V and 100^0C respectively giving energy close to the 'SS' corner. In contrast, for 'FS' corner, voltage and temperature were chosen as 1.98V and 0^0C giving energy close to the 'FF' corner. The values of the voltage and temperature can be interchanged for the skewed corners causing SF corner to be closer to 'FF' and 'FS' corner closer to 'SS'.

Based on the voltage and temperature chosen for the respective corners, the energy per cycle for GF(2^4) implementation using WCS-QuAL, SPGAL and EE-SPFAL were measured at 10MHz and 10fF load capacitance for 10 sets of random inputs. The result of the PVT variations for GF(2^4) implementation are summarized in Table III.

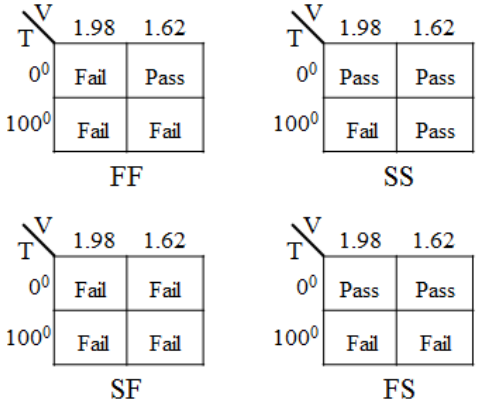

Fig. 6. SPGAL [15],[16] functionality at all Process corners, Voltage and Temperature.

SPGAL implementation fails to provide the correct functionality hence, its value is not measured for 'FF' and 'SF' corners at the chosen voltage and temperature values. Though SPGAL does not suffer from NAL during the evaluation phase of the power-clock, but it suffers from coupling effect. This is because of the absense of cross-coupled nMOS transitors in the latch. Consequently, one of its output nodes remain floating during the evaluation, hold, and recovery phase. Due to this, it gets coupled to the output node following the power clock thus, not allowing it to be at zero value. Accordingly, its zero value remains between 0.8V to 1V. In cascade logic, when the logic zero is passed its value is much higher than the threshold voltage of the evaluation transistors. This causes the wrong value of the signal to propagate and fails to offer the correct functionality of the circuit. The two output nodes are connected to the ground via discharge input only during the idle phase of the power-clock before the next input is evaluated. From Fig. 6, it can be seen that SPGAL failed at all the process corners at different voltage and temperature conditions.

In contrast, EE-SPFAL is the modification of SPGAL. Unlike SPGAL, EE-SPFAL has latch made of two pMOS transistors and two nMOS transistors. The cross-coupled nMOS transistors help one of the output nodes to connect to ground during evaluation, hold, and a part of the recovery phase. Thus, suffers from coupling effect only for a part of recovery phase (below the threshold voltage of the pMOS). EE-SPFAL passed the functionality test for each process corner at different voltage and temperature conditions. Also, on the basis of % NED and % NSD, EE-SPFAL performs better than SPGAL.

On the other hand, WCS-QuAL also passed the functionality test against PVT variations and outperforms EE-SPFAL and SPGAL on the basis of %NED and %NSD as can be seen from Table III.

TABLE III. SIMULATION RESULTS COMPARING THE PERFORMANCE OF GF(2^4) BIT PARALLEL MULTIPLIER

Logic Designs	Process Corners at 10MHz				
	FF V=1.98, T=100^0C	**SS V=1.62, T=0^0C**	**SF V=1.62, T=100^0C**	**FS V=1.98, T= 0^0C**	**TT V=1.8, T=27^0C**
EE-SPFAL					
E_{av}(fJ)	189.83	106.90	97.299	148.00	119.41
%NED	2.227	1.421	2.784	1.688	1.615
%NSD	1.067	0.620	1.454	0.613	0.470
SPGAL					
E_{av}(fJ)		164.69		284.99	218.38
%NED		2.941		2.139	2.061
%NSD	FAIL	1.192	FAIL	1.110	0.678
WCS-QuAL					
E_{av}(fJ)	280.13	173.25	183.32	241.14	189.50
%NED	0.853	0.455	0.587	0.657	0.250
%NSD	0.334	0.240	0.304	0.340	0.129

B. Impact of Power-Clock Supply Scaling.

An easy way of reducing energy in adiabatic logic is by reducing the supply voltage. Energy dissipation has a quadratic dependence on the supply voltage, V_{DD}. But as the power supply is reduced it affects the gate overdrive voltage, V_{GS}-V_{th} and an increase in on-resistance is observed (as on-resistance of the transistors in the charging path is also a function of supply voltage). A more detailed description can be found in [20]. Thus it is important to evaluate the impact of power-clock scaling on secure adiabatic logic designs.

The power-clock was scaled from 1.8V down to 0.5V. The simulation results of the power-clock scaling at 10MHz and 10fF load for 10 random inputs are summarized in Table IV. Since the simulation results for 1.8V power supply were included in Table III, they are omitted in Table IV. It can be seen that SPGAL fails to work at supply voltage less than 0.6V. It is because; Firslty, SPGAL has the nMOS evaluation transistors connected between the power-clock and the output nodes, thus have bulk effect which raises the threshold voltage of the evaluation transistors. When the power-clock is scaled below 0.6V, the output node fails to follow the power-clock as the condition for the transistor to be ON ($V_{GS} > V_{th}$) is not full filled. It is because the source voltage starts rising with the power-clock and the difference between the gate-to-source voltage becomes less than the threshold voltage of the transistor, thus it turns off. Secondly, due to the absence of the cross-coupled nMOS transistors, it suffers from severe coupling effect causing one of the output node to be coupled to the other output node folowing the power-clock. Hence, the circuit fails to deliver the correct functionality.

Though, EE-SPFAL is based on PFAL adiabatic logic and has the nMOS transistors evaluation network connected between the power-clock and the output nodes. But having cross-coupled nMOS transistors and discharging transistors help EE-SPFAL to give correct functionality. Because the discharge transistors keep the output nodes to zero before the evaluation phase of the power-clock, it helps one of the output nodes to held at zero and turn on the pMOS transistor connected to the opposite node to help it follow the power-clock.

TABLE IV. SIMULATION RESULTS COMPARING PERFORMANCE OF GF(2^4) MULTIPLIER AGAINST POWER SUPPLY SCALING

Logic Designs	Power-clock scaling @ 10MHz					
	V=.5	V=.6	V=.8	V=1	V=1.2	V=1.5
EE-SPFAL						
E_{av}(fJ)	31.531	38.13	36.17	45.36	59.00	86.26
%NED	3.138	2.467	1.517	1.601	1.758	1.615
%NSD	1.309	0.877	0.612	0.757	0.602	0.470
SPGAL						
E_{av}(fJ)		32.53	44.03	63.02	91.62	147.1
%NED		4.797	4.210	3.003	2.043	1.699
%NSD	FAIL	2.336	1.561	1.290	0.964	0.712
WCS-QuAL						
E_{av} (fJ)	40.88	51.50	56.57	72.78	95.02	135.9
%NED	0.073	0.097	0.203	0.793	0.884	0.352
%NSD	0.028	0.051	0.107	0.420	0.459	0.186

WCS-QuAL, on the other hand, works well for power supply ranging from 1.8V to 0.5V. This is because it uses dual evaluation network thus, when the power-clock is scaled down to 0.6V and below, as soon as the power-clock starts rising, the output node starts following the power-clock. The nMOS transistors of the evaluation network connected between the power-clock and the output nodes remain ON as long as the condition $V_G - V_S > V_{tn}$ holds true. The transistors are turned OFF, as the power-clock starts rising and the gate-to-source voltage goes below the threshold voltage. At this time, the evaluation network connected between the output nodes and ground will take the control by providing one of the output nodes to held at ground and turning on one of the pMOS transistors and allowing the other output node to follow the power-clock.

From Table IV It can also be seen that WCS-QuAL exhibits the least value of %NED and %NSD than EE-SPFAL and SPGAL. As discussed before, the energy dissipated by WCS-QuAL is more in comparison to EE-SPFAL and SPGAL at output load of 10fF, but as the supply voltage is increased, the energy of WCS-QuAL approaches SPGAL and eventually becomes less at voltage 1.5V. This is because of the coupling effect mentioned before. As the floating node gets coupled to the node following the power-clock, its volatge increases on increasing the supply voltage, causing high current consumption. Consequently, it will never be at ground leading to higher energy dissipation.

C. Evaluation of the Proposed and Existing Logic at TSMC 90nm Technology node.

With the lowering of technology, V_{DD} is reduced. Reduction of power supply reduces the dynamic energy dissipation thus, the main motivation of this section is to evaluate the impact of lower technology on WCS-QuAL, EE-SPFAL, and SPGAL. Simulations for all the secure adiabatic logic designs were performed with Spectre simulator using Cadence EDA tool in a 'typical-typical' 'TT' process corner using TSMC 90nm CMOS process at 1V power supply. The load capacitance chosen was 10fF and the transistor sizes for all the designs were set at (W_n=W_p=100nm, L_n=L_p=100nm). Simulation results for TSMC 180nm and 90nm are summarized in Table V. It can be seen that WCS-QuAL outperforms both the existing logic designs. WCS-QuAL shows the energy reduction of approximately 71.8% when moving from 180nm to 90nm whereas; EE-SPFAL shows nearly 66.2% reduction in energy. Also, it is worth mentioning that in comparison to EE-SPFAL, WCS-QuAL dissipates 58.7% and 32.5% more energy at 180nm and 90nm respectively.

TABLE V. SIMULATION RESULTS COMPARING PERFORMANCE OF GF(2^4) BIT-PARALLEL MULTIPLIER AGAINST TECHNOLOGY

Logic Designs	Technology @ 10 MHz	
	180nm @ 1.8V	90nm @ 1V
EE-SPFAL		
E_{av}(fJ)	119.41	40.350
%NED	1.615	1.410
%NSD	0.470	0.599
SPGAL		
E_{av}(fJ)	218.38	
%NED	2.061	FAIL
%NSD	0.678	
WCS-QuAL		
E_{av} (fJ)	189.50	53.485
%NED	0.250	0.186
%NSD	0.129	0.090

Since SPGAL fails to perform at 90nm technology, no comparison is given. It failed to deliver the correct functionality because of severe coupling effect due to which the output node which should have been at logic zero, reaches close to 1V. For instance, at 180nm technology, with $V_{tn} \approx 0.5V$ and $|V_{tp}| \approx 0.55V$, the output nodes which were supposed to be at 'zero' logic level were at 0.67V approximately. This is above the threshold voltage and can lead to functionality failure in cascaded logic in a large adibatic system.

Whereas, in 90nm technology with $V_{tn} \approx 0.34V$ and $|V_{tp}| \approx 0.35V$, the output nodes which were supposed to be at zero logic level were at approximately 0.7V and logic 'one' was at about 0.89V for 1V power supply. The value for logic 'zero' is much higher than the threshold voltage of the transitors and is close to power supply. Thus, in a cascade logic, could turn on the transitors which should be off and fail to offer the correct functionality.

VI. Conclusion

In this paper, we evaluate and compare the performance of WCS-QuAL, EE-SPFAL, and SPGAL at frequency ranging from 1 MHz to 100MHz. Simulation results show that on the basis of %NED and %NSD, WCS-QuAL outperforms EE-SPFAL and SPGAL at all simulated frequencies. Also, all the 2-input gates using WCS-QuAL dissipates approximately equal energy making its energy dissipation logic operation independent. Moreover, WCS-QuAL dissipates approximately same energy as by EE-SPFAL and SPGAL at the output load capacitance over 100fF.

These results were confirmed by using GF (2^4) bit-parallel multiplier as a design example for evaluation and comparison. The impact of PVT variations, power supply scaling and technology on the performance of the three logic designs was investigated. Simulation results show that WCS-QuAL passed the functionality test against PVT variations and power supply scaling. It exhibits the least value of %NED and %NSD against PVT variations and when the power supply is scaled from 1.8V to 0.5V in comparison to EE-SPFAL and SPGAL. In comparison to EE-SPFAL, WCS-QuAL shows 5% more energy reduction when moving from 180nm to 90nm technology. At 90nm technology, the difference in energy dissipation between WCS-QuAL and EE-SPFAL is reduced compared to the energy dissipation at 180nm.

Acknowledgment

The authors wish to thank the 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] T. Popp, S. Mangard, E. Oswald, "Power Analysis Attacks and Countermeasures", IEEE Design & Test of Computers, vol. 2, no. 6, pp. 535 – 543, 2007.

[3] Thomas S Messerges, Ezzat A Dabbish, and Robert H Sloan. Examining smart-card security under the threat of power analysis attacks. Computers, IEEE Transactions on, 51(5):541–552, 2002.

[4] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan. Investigations of power analysis attacks on smartcards. Smartcard, 99:151–161, 1999.

[5] 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.

[6] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," in Proc. ESSCIRC, Paris, France, 2004, pp. 246-251.

[7] T. Popp and S. Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints", in Proc. CHES, Edinburgh, UK, 2005, pp. 172-186.

[8] Z. Chen and Y. Zhou, "Dual-rail random switching logic: A countermeasure to reduce side channel leakage", in Proc. CHES, Yokohama, Japan, 2006, pp. 242-254.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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, 2016.

[16] S. D. Kumar, H. Thapliyal, A. Mohammad, V. Singh, and S. K. Perumalla, "Energy-efficient and secure s-box circuit using symmetric pass gate adiabatic logic," in Proc. IEEE computer society Annual Symposium on VLSI (ISVLSl), 2016.

[17] S. D. Kumar, H. Thapliyal, "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, no. 99, 2016.

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

[19] K. Tiri, "Side-channel attack pitfalls," ACM/IEEE DAC, pp. 15-20, 2007.

[20] Philip Teichmann. Adiabatic logic: future trend and system level perspective, vol. 34. Springer Science & Business Media, 2011.

[21] F. Mac´e, F.-X. Standaert, J.-J. Quisquater, Information Theoretic Evaluation of Side-Channel Resistant Logic Styles, CHES 2007, Lecture Notes in Computer Science, vol 4727, pp 427-442, Vienna, Austria, September 2007.

[22] E. Tena-Sanchez, J. Castro, and A. J. Acosta, "A Methodology for ´ Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 4, no. 2, pp. 203-215, Jun. 2014.