Investigating the effectiveness of Without Charge-Sharing Quasi-Adiabatic Logic for energy efficient and secure cryptographic implementations

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

Investigating the Effectiveness of Without Charge-Sharing Quasi-Adiabatic Logic for Energy Efficient and Secure Cryptographic Implementations

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—**Existing secure adiabatic logic designs use charge sharing inputs to deliver input independent energy dissipation and suffer from non-adiabatic losses (NAL) during the evaluation phase of the power-clock. However, using additional inputs present the overhead of generation, scheduling, and routing of the signals. Thus, we present "Without Charge-Sharing Quasi-Adiabatic Logic", WCS-QuAL which doesn't require any charge sharing inputs and completely removes the NAL. The pre-layout and post-layout simulation results of the gates show that WCS-QuAL exhibits the lowest Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) against all process corner variations at frequencies ranging from 1MHz to 100MHz. It also shows least variations in average energy dissipation at all five process corners. The simulation results show that the 8-bit Montgomery multiplier using WCS-QuAL exhibits the least value of NED and NSD at all the simulated frequencies and against power-supply scaling and dissipates the lowest energy at frequencies ranging from 20MHz to 100MHz.**

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

1. INTRODUCTION

In the present information and communication technology based world, security of the information is a fundamental requirement. Security is usually ensured by cryptography algorithms which are based on hard-to-solve mathematical problems. However, mathematically strong cryptographic algorithms are often unable to provide complete security due to the advent of Side Channel Attacks (SCA).

A class of SCA which is particularly powerful is the Power Analysis Attack (PAA). PAA such as Differential Power Analysis (DPA) [1-2] has become a major threat to the security of cryptographic implementations. DPA attacks involve statistical and digital processing techniques on a large number of monitored power traces.

Hiding [3] and masking [4] are the most common methods of resistance used at the gate level. The objective of hiding is to make the power consumption of the cryptographic device independent of the data processed. Masking, on the other hand, relies on randomizing the input/key dependent intermediate values processed during the execution of the cryptographic device.

This paper is organized as follows; in section 2, background and motivation for this paper are presented. Contributions of this paper are presented in section 3. Existing logic designs are discussed in section 4. WCS-QuAL is presented in section 5. In section 6, simulation results of the logic gates and 8-bit Montgomery Multiplier using WCS-QuAL and existing logic are presented. Finally, the paper is concluded in section 7.

2. BACKGROUND & MOTIVATION

There are numerous papers that have addressed the design of PAA resistant logic designs such as Masked Dual-rail Pre-charge Logic (MDPL) [5] and Dual-rail Random Switching Logic (DRSL) [6] are the combination of the masking scheme and the dual-rail pre-charge logic. However, it has been shown [7] that due to the problems like glitches, and detection of the value of the mask bits, the masking logic styles only slightly increase the number of patterns required to achieve a successful attack. Sense-Amplifier-Based Logic (SABL) [3] and Wave Dynamic Differential Logic (WDDL) [8] are dual-rail pre-charge logic styles [9]. However, SABL requires a full-custom design tool to equalize the capacitances of the two differential outputs. WDDL [8], was designed to avoid the use of full custom design tool. However, its data-dependent time of operation made it susceptible to timing attacks [9] Three-phase Dual-rail pre-charged logic (TDPL) [10] is based on a three-phase operation and needs an additional discharge phase after pre-charge and evaluation phase. However, TDPL gate requires three control signals, and thus, needs a separate unit to generate and schedule control signals in order to prevent glitches. All of these countermeasures applied conventional CMOS logic operation and thus are not energy efficient.

There are several, adiabatic logic designs [11], [23] resilient to PAA such as CSSAL [12], SyAL [13], and SQAL [14]. These logic styles use charge-sharing and output load balancing at two output nodes to deliver constant energy consumption. SyAL and SQAL are based on Efficient Charge Recovery Logic (ECRL) [15]. SyAL uses more number of charge sharing transistors compared to SQAL. CSSAL is based on 2N-2N2P adiabatic logic [16] and is an improvement over SyAL. CSSAL consumes more energy, has a complex structure. As SyAL and SQAL use charge sharing input and CSSAL uses Charge sharing and evaluation input thus presents the overhead of generation, scheduling, and routing of the additional inputs.

As the abstraction level is decreased, new flaws may appear in the design, which can increase the amount of information leaked to the attacker [17]. A countermeasure that is secure at a high abstraction level may not be secure when power supply scaling, load capacitances, process variations, frequency of operation are considered [18]. Process variations can worsen the resistance of secure logic designs against PAA and thus, can cause the design to fail [24]- [26]. Therefore, it is important to evaluate the performance of WCS-QuAL and existing logic against process corner variations, which this work reported in this paper, is dedicated to.

In adiabatic circuits, Adiabatic Losses (AL) increase as the frequency of operation is increased (steeper slope). Therefore, it would be worth evaluating the impact of frequency on the performance of WCS-QuAL and existing logic designs.

Constant power consumption in secure adiabatic logic designs is guaranteed by charge-sharing and output nodes load balancing. In schematic design, the resistances and capacitances of the wires are not taken into consideration. Therefore, it is important to analyze and evaluate the effect of resistances and capacitances of the wires on NED and NSD through post-layout simulations.

It is also important to evaluate the performance of WCS-QuAL and existing logic in a complex system. Thus, for comparison and evaluation, an 8-bit Montgomery multiplier using WCS-QuAL, CSSAL, SQAL, and SyAL were implemented as an application example.

WCS-QuAL has been compared with existing techniques namely SyAL, SQAL [13],[14] and CSSAL [12] and not with other dual-rail pre-charge logic designs and masked logic designs because the later works with the need for a DC power supply, unlike adiabatic logic that works with a slowly changing AC power supply and thus are energy efficient.

3. CONTRIBUTIONS

The focus of this paper is to evaluate and compare the performance of WCS-QuAL and existing logic against frequency variations, process corner variations, power supply scaling and the effect of the resistances and capacitances of the interconnect wires on the balancing of the output nodes and on the NED and NSD after layout designs. Also, 8-bit Montgomery multiplier is implemented as a representative example for cryptography applications to further evaluate and compare the performance.

The main contributions of this paper are as follows:

- WCS-QuAL doesn't require any charge-sharing between the output/internal nodes thus saving the overhead of generation, scheduling, and routing of additional inputs.
- WCS-QuAL also completely removes the NAL during the evaluation phase of the power-clock and reduces coupling effect.
- The performance (on the basis of NED and NSD) of the existing secure adiabatic logic changes with the frequency of operation whereas; the performance of WCS-QuAL is frequency independent.
- Energy dissipation of WCS-QuAL exhibits least sensitivity to process corner variations.
- All 2-input gates using WCS-QuAL dissipates almost equal energy thus; making it difficult to identify which logic operation is being performed.
- WCS-QuAL exhibits the lowest energy dissipation from frequencies 20MHz to 100MHz.

4. EXISTING CHARGE SHARING LOGIC DESIGNS

Charge sharing is done to remove the remaining charge (due to NAL in quasi-adiabatic logic) from the output nodes before the evaluation of the next input takes place. Charge sharing transistors are turned ON during the idle phase of the power-clock. The NOT/BUF gate using SQAL and SyAL has identical structure. Fig. 1(a) and (b) shows the schematic of the SyAL/SQAL and CSSAL NOT/BUF gate respectively.

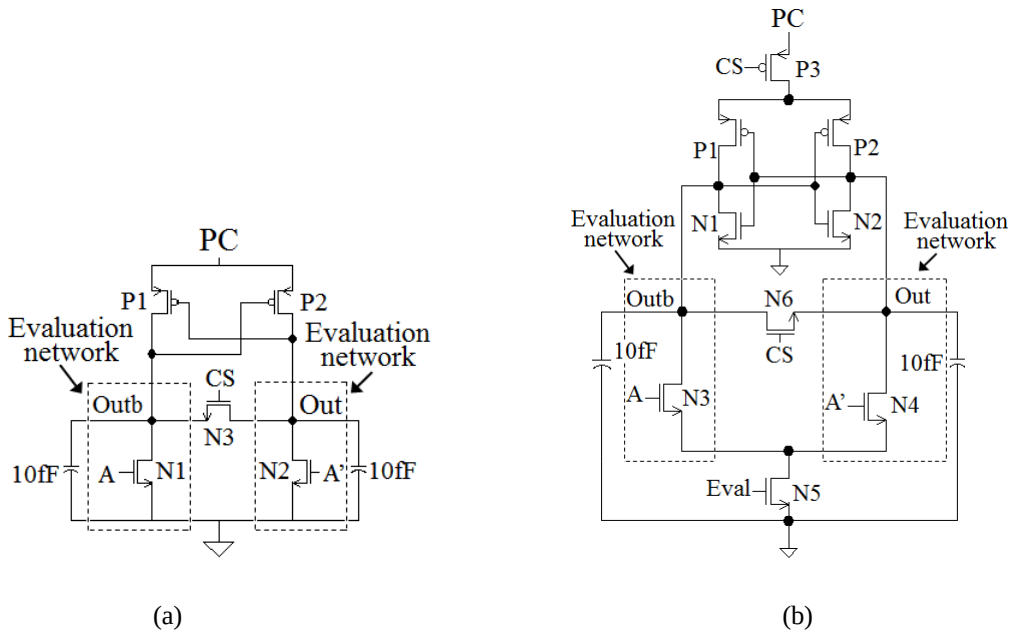


Fig. 1. (a) SyAL/SQAL NOT/BUF [13],[14] schematic (b) CSSAL NOT/BUF [12] schematic.

From Fig. 1(a), It can be seen that N1 and N2 are the input transistors, N3 is the charge sharing transistor and transistors, P1 and P2 forms the cross coupled latch that helps to hold the two output nodes 'Out' and 'Outb' during the hold phase of the Power-Clock (PC). The evaluation networks are connected between the two output nodes and the ground.

During the evaluation phase of the PC, When the input, A is logic '1' (and A' is logic '0') and the PC ramps up from zero to V_{DD}, the output node, 'Outb' is connected to the ground through transistor N1 and the output node 'Out' will follow the PC through the pMOS transistor, P2, when the PC has reached above the threshold voltage of the transistor P2. For the duration, when the PC is below the threshold voltage, the

output node ‘Out’ will stay at logic ‘0’ and will abruptly start following the PC when it reaches above the threshold voltage. This is termed as Non Adiabatic Loss (NAL). Working of SyAL and SQAL can be found in [13] and [14].

In Fig. 1(b), N3, N4 are the input transistors, N6, P3 are the charge sharing transistors, N5 is the evaluation transistor and P1, P2 and N1, N2 forms the cross coupled latch responsible for holding the two output nodes ‘Out’ and ‘Outb’ during the hold phase of the Power-Clock (PC). The evaluation networks are connected between the two output nodes and the evaluation transistor, N5.

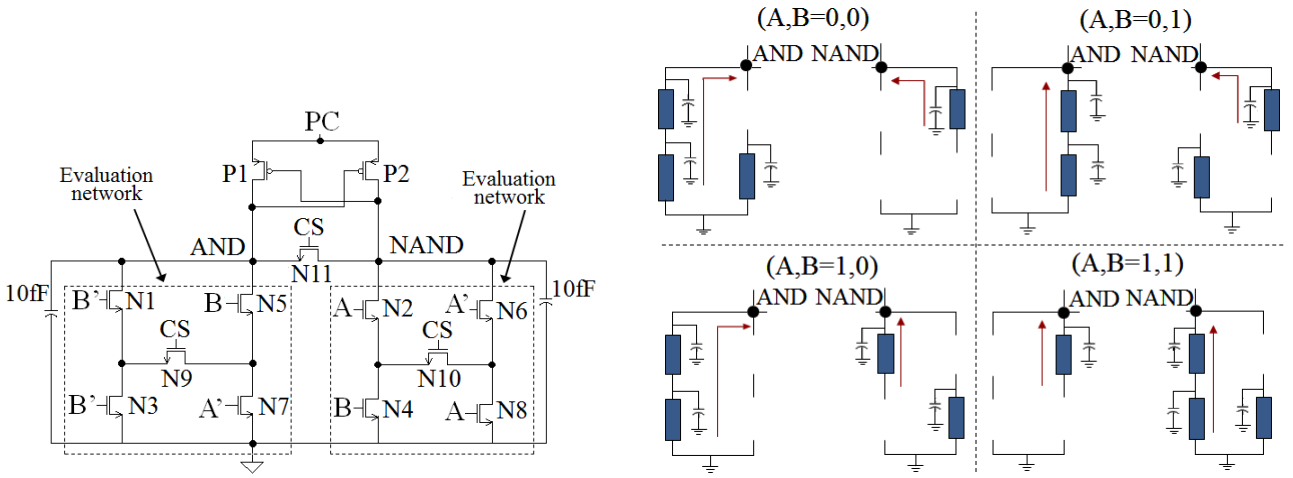
Like SyAL and SQAL, CSSAL also suffers from NAL during the evaluation phase of the PC. Also, due to the charge sharing transistor, P3, the output nodes will suffer increased lag in following the power-clock and thus have higher NAL and dissipates more energy.

If the charge sharing transistor, CS is removed in SQAL, SyAL and CSSAL, the charge will remain trapped on the evaluating output node. For instance, From Fig 1(a), for the condition when input A is logic ‘1’ during the idle phase, the output node, ‘Outb’ will be connected to ground through transistor N1. Whereas, the output node ‘Out’ will have the left-over charge on it in the absence of charge sharing input. When in the next PC cycle, if the input does not change, the same condition will arise. The leftover charges on the output node, ‘Out’ can be discharged to zero if the inputs changes in the next cycle.

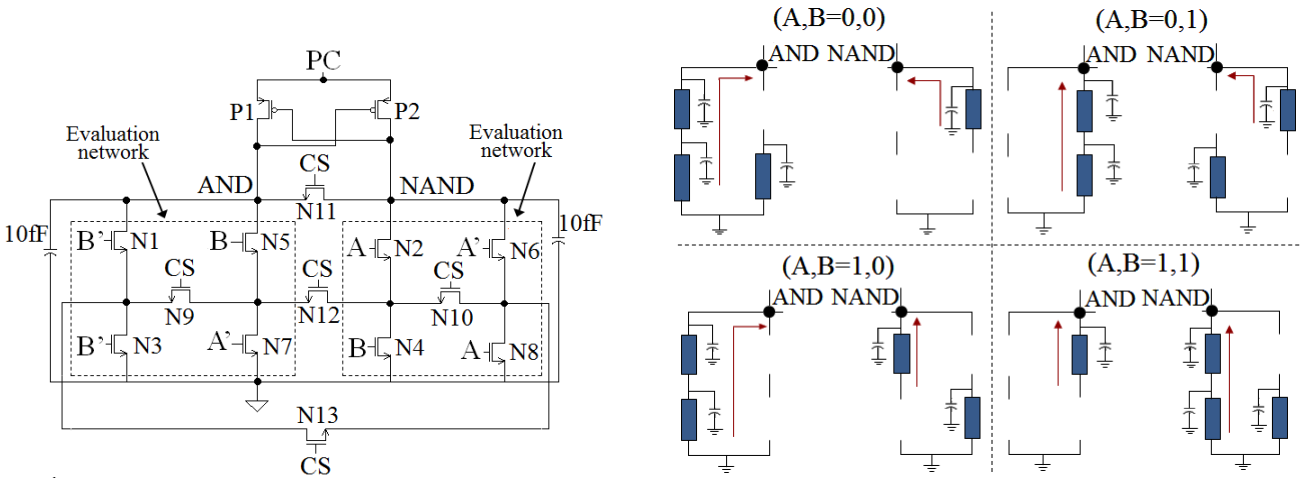
The AND/NAND gate and their equivalent RC models of the internal nodes for SQAL, SyAL, and CSSAL during the evaluation phase are shown in Fig. 2 (a), (b) and (c) respectively. It can be seen that for each of the four input combinations, the output node capacitance is slightly different. This gives data-dependent behavior leading to PAA vulnerability. For instance, from Fig. 2(a) it can be seen that for input combination AB= ‘00’, output node, AND has three transistors ON whereas, NAND has one transistor ON. For AB= ‘01’ and ‘10’, the output nodes, AND/NAND each have two transistors ON. For AB= ‘11’, output

node, AND has one transistor ON whereas, NAND has three transistors ON. This holds true for Fig. 2(b) and (c) also. This makes the power consumption of the existing logic designs data dependent.

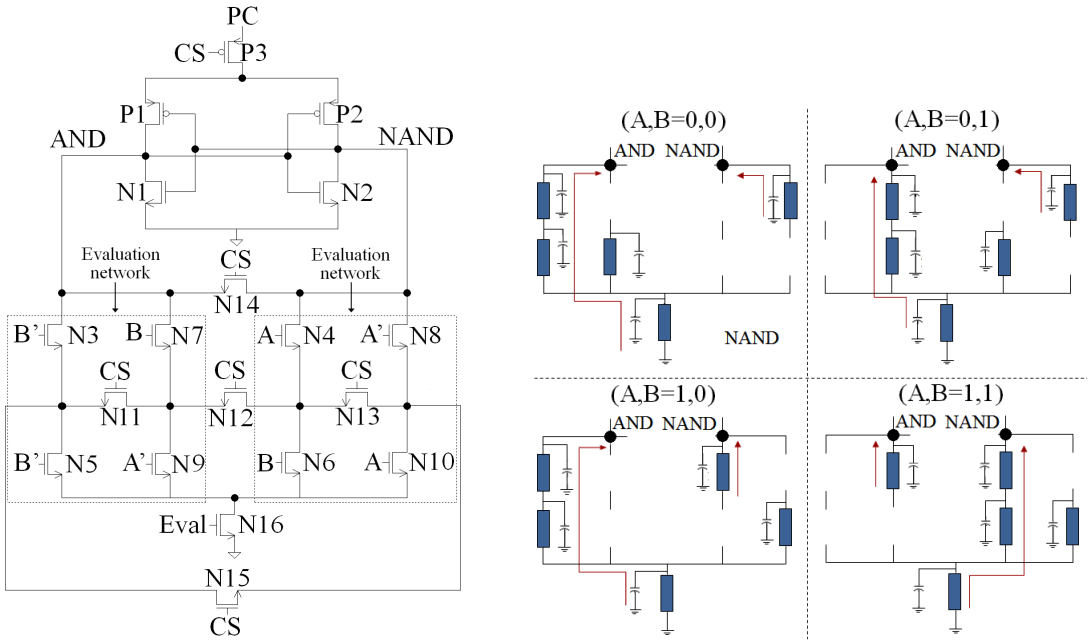
It should also be noted that due to the absence of cross-coupled nMOS transistors, both SQAL and SyAL suffer from coupling effect during the recovery phase of the power-clock.



(a)



(b)



(c)

Fig. 2. Equivalent RC models of AND/NAND gates using (a) SQAL[14] (b) SyAL[13] (c) CSSAL[12] during evaluation phase.

5. WCS-QuAL Based Logic Gates

For data-independent power consumption, the two output nodes of the adiabatic gate should have equal capacitance (equal number of 'ON' transistors) charged for each input transitions. This can be achieved by having symmetric structure, where equal number of transistors is 'ON' on both the output nodes for each input transition. In proposed logic, this is achieved by 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 the ground as shown in Fig. 3(a). This allows equal number of transistors to be ON in the diagonally opposite evaluation networks on the two output nodes for each input transition. Having dual duplicate evaluation network helped making the circuit symmetric and getting the data-independent power-consumption. It also helps the two output nodes to discharge to zero (without using charge sharing input) before the evaluation of the next inputs. For instance, From Fig. 3(a) and (b) during the idle phase, when A is one (A' is zero) the output node Out is connected to the PC which is zero and the output node Outb to ground and therefore, the two output nodes are discharged to zero without the need of charge sharing input before the

evaluation phase. If the input A does not change and remains one in the next cycle of the PC still the charges on the output node, Out will be discharged to zero in the similar manner. This contrasts with the other structures which require a “charge-sharing” transistor to achieve the same effect.

Figure 3(a) and (b) shows a NOT/BUF gate using WCS-QuAL and its timing diagram respectively. The operation of WCS-QuAL gate is explained through the design of a buffer. 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, ‘Out’ and ‘Outb’ to their respective voltages. The timing diagram shows the PC, input A, its complement A’ and the output nodes ‘Out’ and ‘Outb’. WCS-QuAL works on 4-phase power-clocking scheme. The operation is explained for A= ‘1’, A= ‘0’:

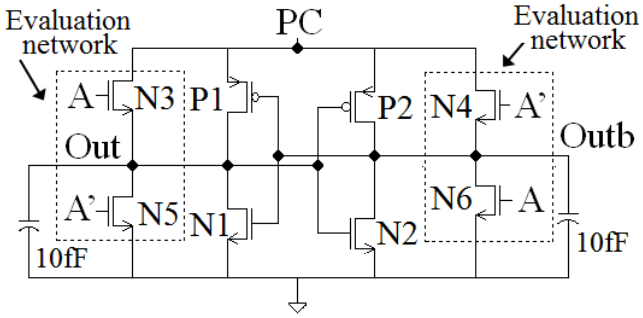
During the Idle phase (I) when input A is rising transistors N3 and N6 are turned ON after the input reaches the threshold voltage. The PC is at logic ‘0’ during the idle phase, therefore, the output node ‘Out’ is connected to PC through transistor N3 and is at zero. Similarly, transistor N6 causes the output node, ‘Outb’ to connect to ground. This way, two output nodes are discharged to zero before the evaluation phase of the power-clock begins. Therefore, no charge sharing transistors are required and the overhead of generation and routing of the 4 phases of the charge sharing input is saved.

During the Evaluation phase (E), input A is one (A’ is zero) and the PC ramping from zero to V_{DD}. The Output node, ‘Out’ follows the PC through N3 and P1 from 0 to V_{DD}-V_{tn} and V_{tp} to V_{DD} respectively and thus, does not suffer from NAL.

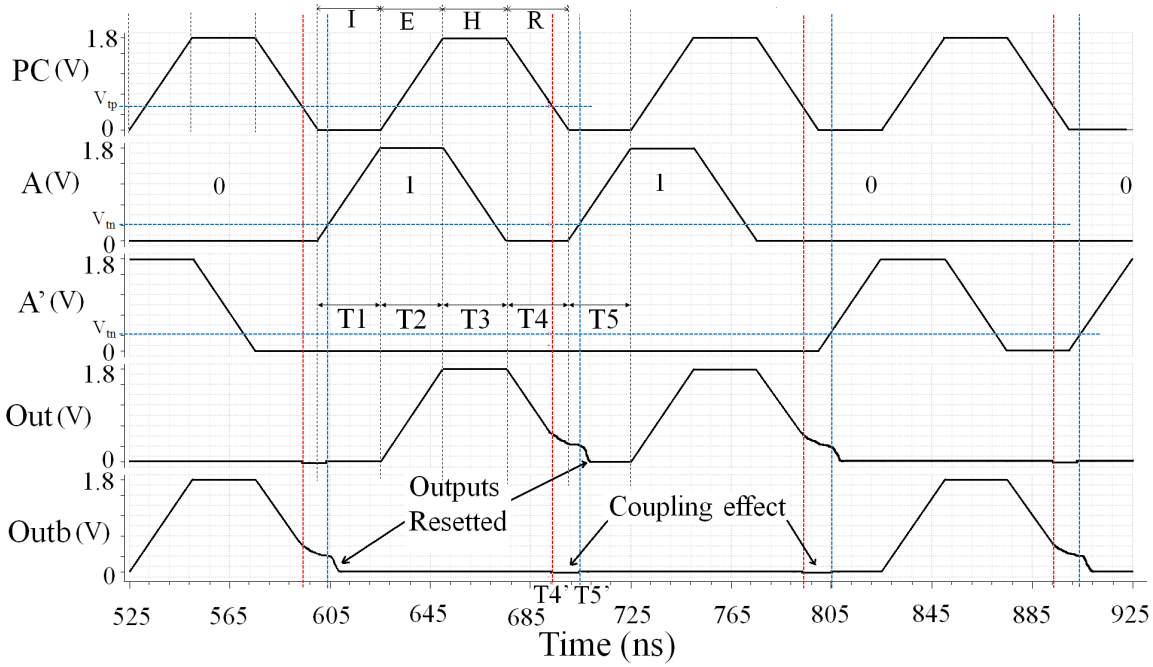
During the Hold phase (H), transistor, N3 is switched off when the gate-to-source voltage falls below V_{tn} and the output nodes ‘Out’ and ‘Outb’ are held at their respective voltages due to the cross-coupled transistors (P1, P2, and N1, N2).

During the Recovery phase (R), the charge on ‘Out’ node is recovered back to the power-clock through the transistor, P1. The charge is recovered till P1 reaches its threshold voltage, $|V_{tp}|$. 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 at time T5’ when the next input arrives, and its gate voltage exceeds the threshold voltage (V_{tn}). From T4’ to T5’, the output nodes are floating, thus the complementary node ‘Outb’ goes below zero voltage due to the coupling effect. Thus, WCS-QuAL suffers from coupling effect only for the duration of T4’ to T5’.



(a)



(b)

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

Fig. 4 (a), (b) and (c) shows the schematics of WCS-QuAL, OR/NOR, XOR/XNOR and AND/NAND, gates respectively. Equivalent RC models of the internal nodes for AND/NAND gate for 4 input combinations during the evaluation phase are shown in Fig. 4 (d). It can be seen that the two output nodes

are balanced and load capacitance at two output nodes is same for each input combinations unlike SyAL, SQAL, and CSSAL. All the 2-input logic have the same structure and an equal number of transistors, except the position of the input signals.

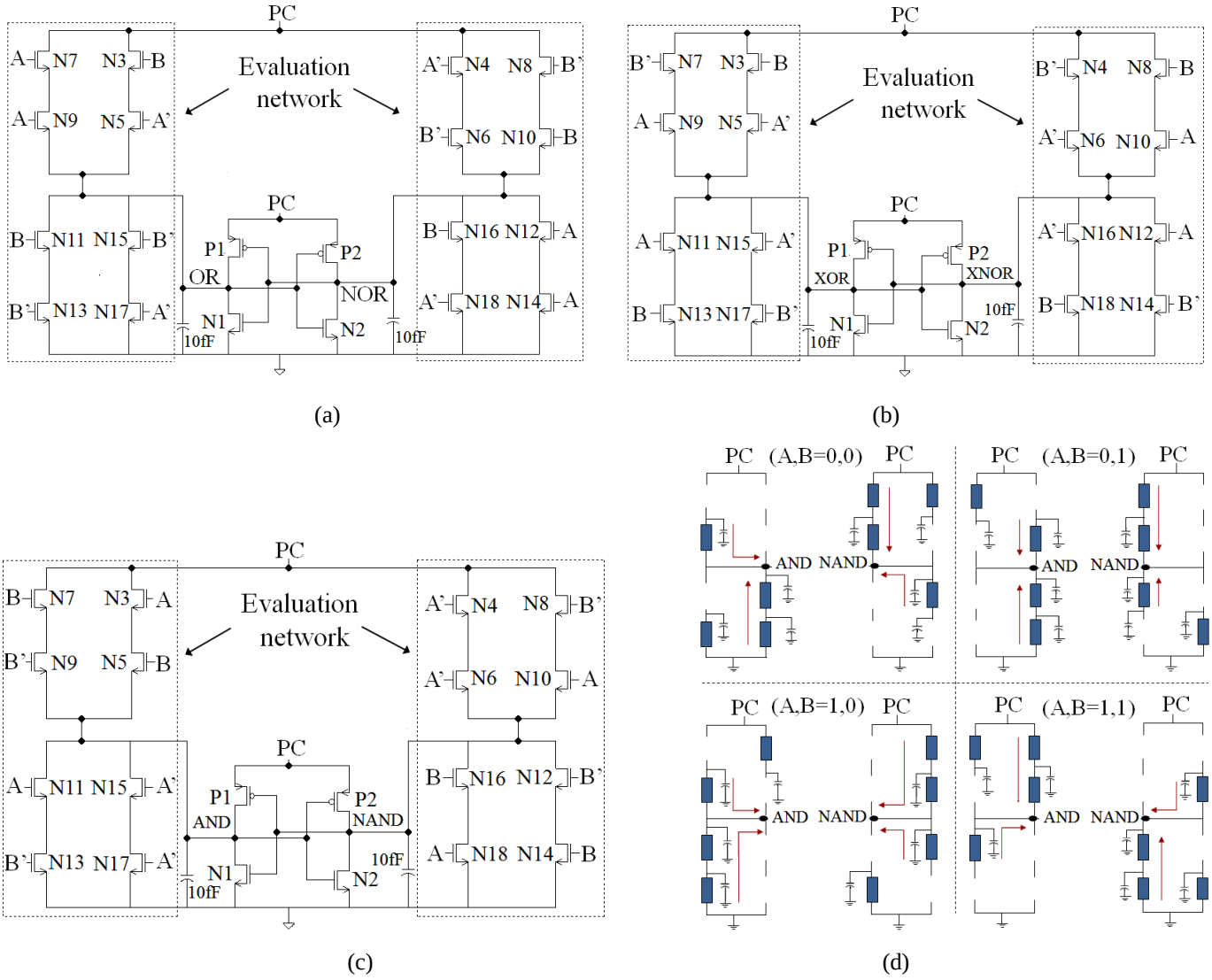


Fig. 4. WCS-QuAL (a) OR/NOR (b) XOR/XNOR. (c) AND/NAND gate (d) Equivalent RC model for evaluation phase.

6. 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 was chosen as 10fF and the transistor sizes for all the designs were set at the technology minimum ($W_{min}=W_n=W_p=220nm$, $L_{min}=L_n=L_p=180nm$).

6.1 Impact of frequency on NED and NSD

The simulations were performed at 1MHz, 10MHz and 100MHz frequencies. The energy dissipation was measured per cycle for 4 and 16-input transitions for NOT/BUF and 2-input gates for SyAL, SQAL, CSSAL, and WCS-QuAL.

The pre-layout simulation results of the evaluated gates are summarized in Table I. We measured the maximum energy (E_{max}), minimum energy (E_{min}), the average energy (E_{av}), and the standard deviation (σ) for single and 2-input gates. Normalized Energy Deviation (NED) and Normalised Standard Deviation (NSD) are obtained according to (1) and (2).

The NED is defined as:

$$NED = \left(E_{\max} - E_{\min}\right)/E_{\max} \tag{1}$$

NSD [12] is defined as:

$$NSD = \sigma/E_{av} \tag{2}$$

Standard Deviation is defined as:

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

Table I shows that WCS-QuAL exhibits the best (i.e. least) value of %NED and %NSD at all simulated frequencies than the existing logic designs.

It also shows that 2-input gates using WCS-QuAL dissipate more energy than the 2-input gates using SQAL and SyAL and slightly less than CSSAL. However, former suffers from NAL only during the recovery phase, whereas, all the three-existing logic suffer from NAL in both the evaluation and recovery

phase of the power-clock. Also, CSSAL has 2 stacked transistors in evaluation and recovery path (as shown in Fig. 1 (b)) thus, has higher NAL than SQAL and SyAL.

At low frequency, the energy dissipated by the adiabatic logic, in general, is dominated by leakage energy and not by Adiabatic Losses (AL) and NAL [21]. Hence, having more number of transistors in WCS-QuAL, than SQAL and SyAL dissipates more energy at lower frequency. On the other hand, CSSAL has approximately equal transistors compared to WCS-QuAL but has higher NAL thus, consumes more energy at all frequencies.

The NOT/BUF gate using WCS-QuAL consumes the lowest energy at all the simulated frequencies. Because the existing logic suffers from NAL in the evaluation phase they exhibits more peak current (Fig. 5(a)) hence dissipate more energy than WCS-QuAL.

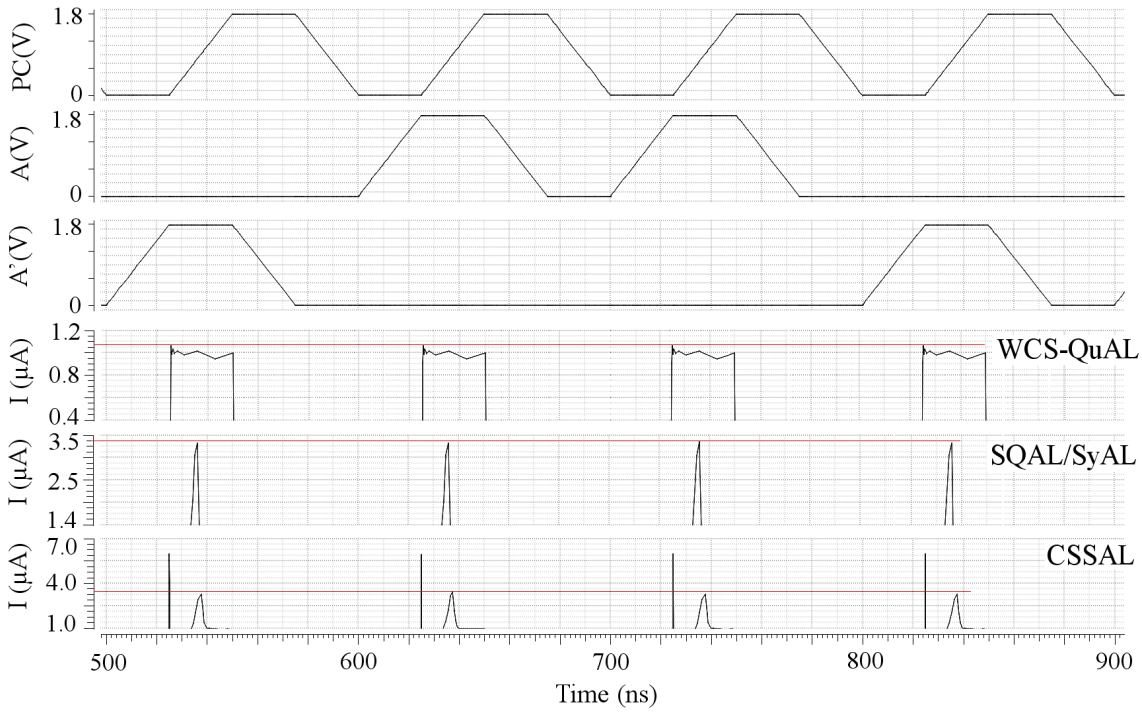
At higher frequencies (short ramping time), the effect of Adiabatic Loss (AL) is more prominent rather than leakage loss [21]. As the frequency is increased, AL combined with NAL leads to more energy dissipation in existing logic designs than WCS-QuAL as can be seen from Table I.

Table I also shows that the performance (based on %NED and %NSD) of existing logic designs changes with frequency. CSSAL is second best followed by SyAL and SQAL at 1MHz, whereas, at 10MHz, SyAL is second best followed by CSSAL and SQAL. The order of performance at 100MHz is same as at 1 MHz. Therefore, the performance (security level) of the existing logic is frequency dependent.

Logic Designs	CSSAL [12]			SQAL [14]			SyAL [13]			WCS-QuAL		
	1 MHz	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*
NOT/BUF												
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

TABLE I. PRE-LAYOUT SIMULATION RESULTS OF GATES USING THE WCS-QuAL AND EXISTING LOGIC

The current waveform for 4-input transitions for NOT/BUF and 16-input transitions for AND/NAND gate for all the four secure logic designs are shown in Fig. 5 (a) and (b). The complementary signals, A’ and B’ for AND/NAND are not shown for simplicity but follows adiabatic principal. The current peaks are given for a power-clock frequency of 10MHz. It can be seen that the proposed logic shows almost least variation compared to the existing logic designs. Also, the peak value of the current is less, resulting in less energy as shown in Table I.

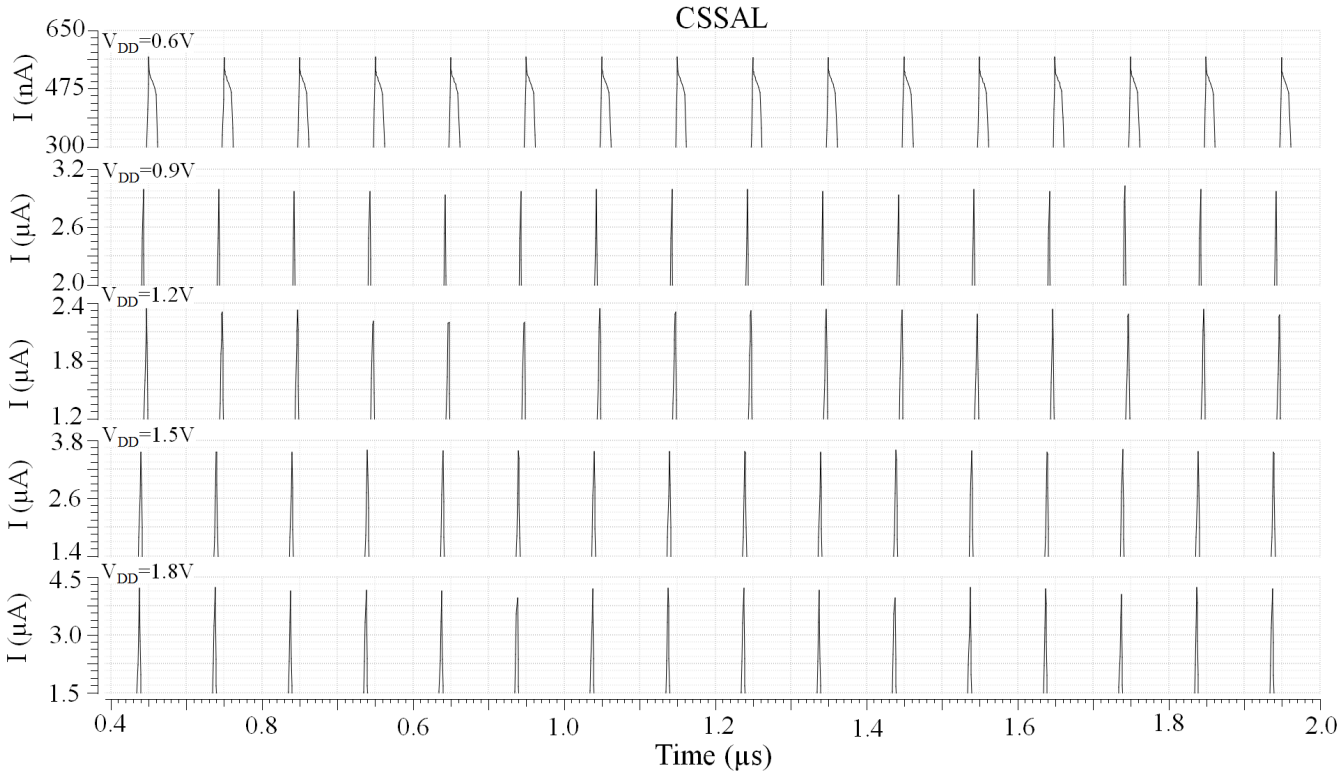


(a)

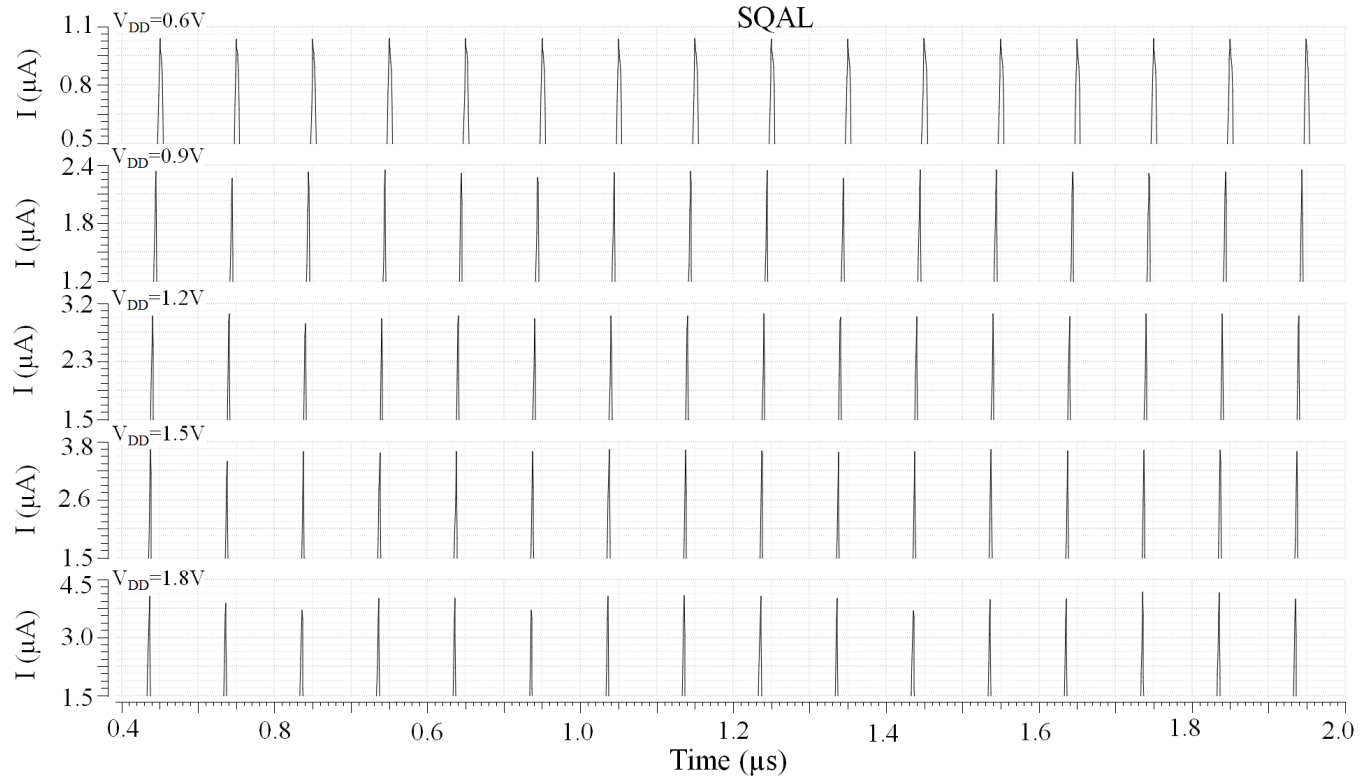
(b)

Fig. 5. The current peaks at 10MHz (a) 4-input transitions for NOT/BUF gate (b) 16-input transitions for AND/NAND gate.

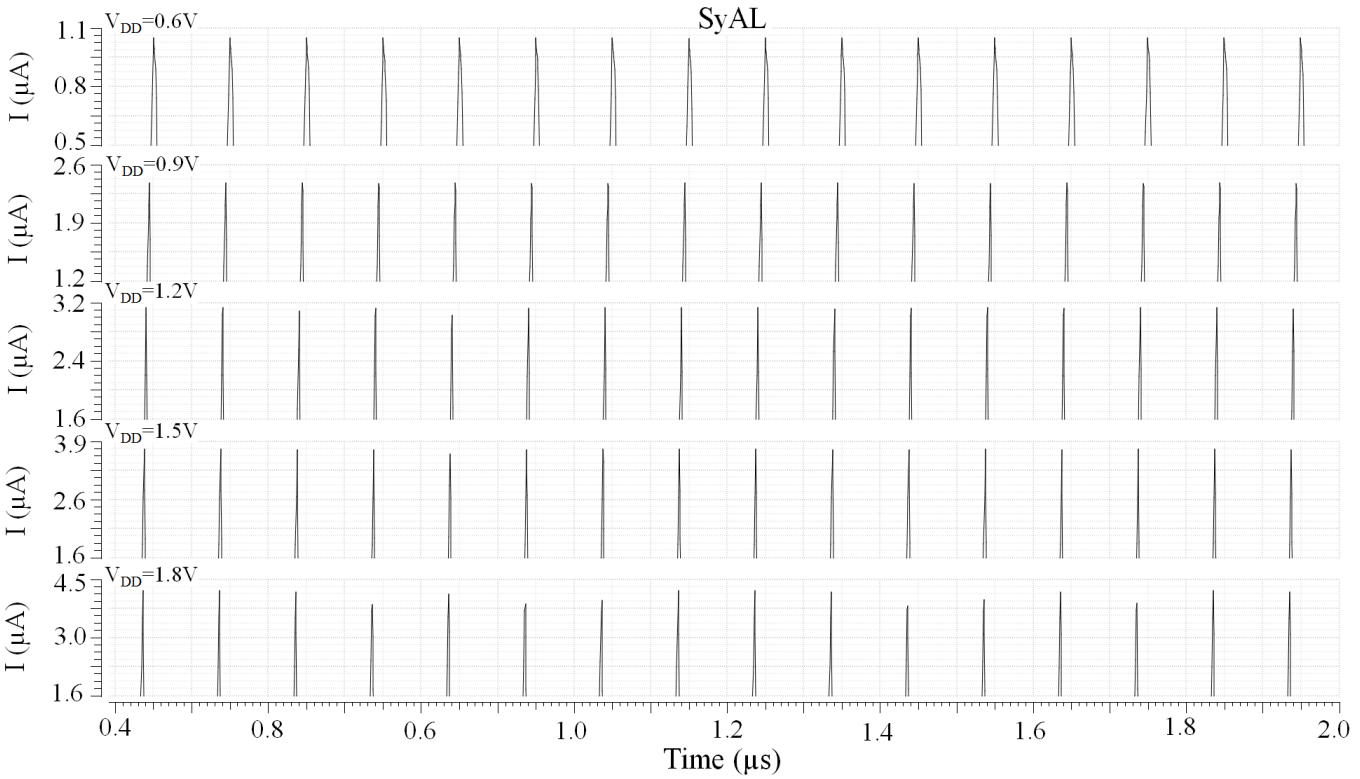
Fig. 6 (a), (b), (c) and (d) shows the current peaks for 16-input transitions in AND/NAND gate, using CSSAL, SQAL, SyAL and WCS-QuAL respectively. The current peaks are shown for power clock ramping from 0V to V_{DD}, where V_{DD} is scaled to 0.6V, 0.9V, 1.2V, 1.5V and 1.8V at 10MHz. It can be seen that WCS-QuAL shows the least variations in comparision to the existing secure adiabatic logic designs at all power-clock values.



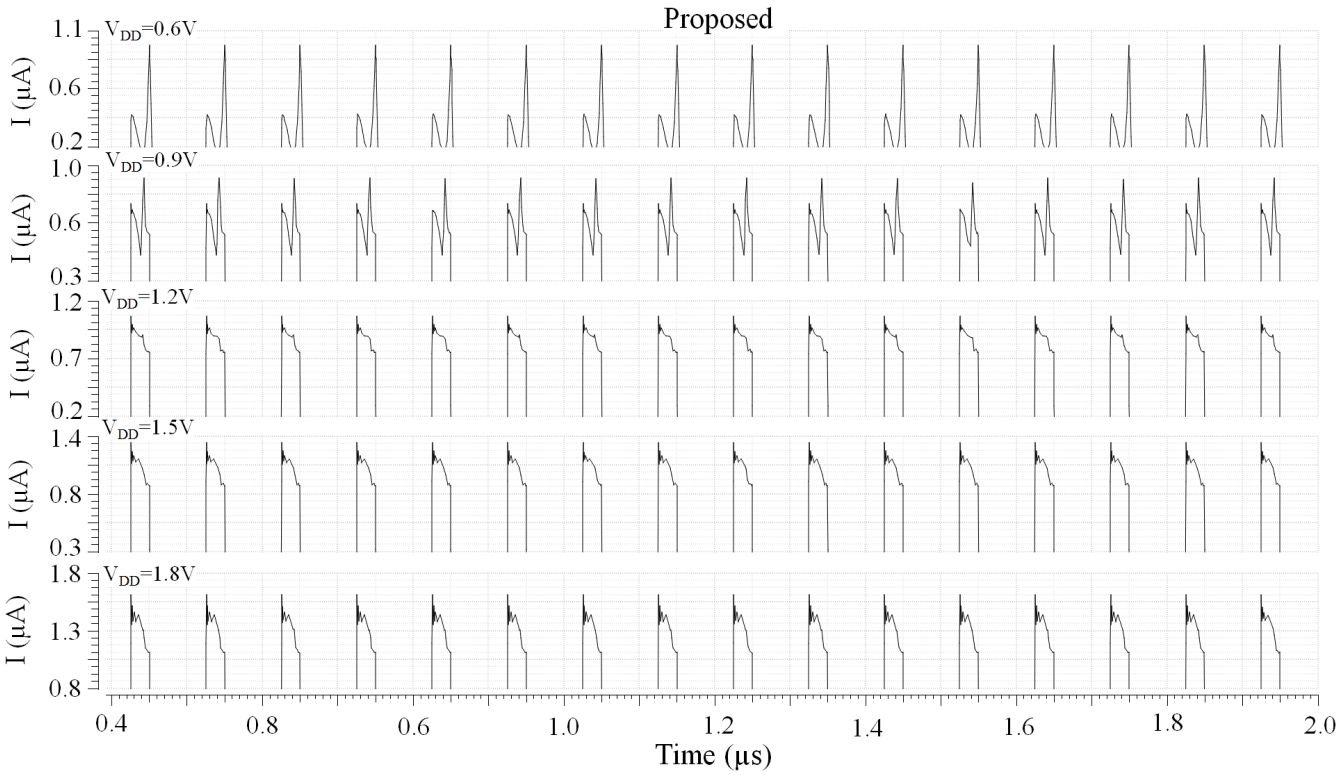
(a)


SQAL
V_{DD}=0.6V
V_{DD}=0.9V
V_{DD}=1.2V
V_{DD}=1.5V
V_{DD}=1.8V
I (µA)
Time (µs)

(b)


SyAL
V_{DD}=0.6V
V_{DD}=0.9V
V_{DD}=1.2V
V_{DD}=1.5V
V_{DD}=1.8V
I (µA)
Time (µs)

(c)



(d)

Fig. 6. Impact of power-supply scaling on the current peaks for 16-input transitions for AND/NAND gate at 10MHz.

6.2 Logic operation independent energy dissipation

Another advantage of WCS-QuAL is that all its 2-input gates dissipate nearly the same energy at all simulated frequencies. Since PAA is based on the principle that where energy consumption is data-dependent, sensitive data can be inferred from analysis of the power supply currents. The main benefit of the logic reported, is that any logic gate's energy consumption is data-independent.

However, an additional level of protection is offered by ensuring, as far as possible, that an AND gate, say, uses the same energy as an OR gate; thereby making it difficult to infer what logic operation is being performed at any one time. In other words, we achieve "gate-independence" as well as data-independence. 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 existing logic. It also shows the standard deviation (σ) of average energy dissipated by the three logic gates at all the simulated frequencies. WCS-QuAL shows the lowest value of standard deviation compared to existing logic designs at all frequencies simulated.

Logic Designs	CSSAL[12]			SQAL[14]			SyAL[13]			WCS-QuAL		
	1 MHz	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*
AND/NAND Eav (fJ)	6.500	10.350	28.710	4.892	7.137	17.870	5.434	7.760	19.235	5.837	6.438	10.674
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
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
Eav,gates(fJ)	6.500	10.360	28.713	4.978	7.211	17.600	5.437	7.762	19.234	5.838	6.439	10.674
σ (fJ)	0.002	0.010	0.005	0.150	0.135	0.441	0.005	0.002	0.001	0.001	0.001	0.001

TABLE II. COMPARISON OF STANDARD DEVIATION OF AVERAGE ENERGY DISSIPATED BY 2-INPUT GATES MEASURED FROM PRE-LAYOUT SIMULATIONS.

6.3 Impact of Process Corner Variations

To further evaluate the robustness of WCS-QuAL, CSSAL, SQAL, and SyAL against process corner variations. The simulations were performed at 'Fast-Fast' (FF), 'Slow-Slow' (SS), 'Fast-Slow' (FS) and 'Slow-Fast' (SF) process corners. The pre-layout simulation results for FF and SS process corners are summarized in Tables III. The simulation results are only tabulated for FF and SS corners as these are the worst and the best-case scenarios. The simulation results show that WCS-QuAL exhibits the least (i.e. best) value of %NED and %NSD for each process corner at frequencies ranging from 1MHz to 100MHz. However, the ranking of performance (level of security based on %NED and %NSD) of CSSAL, SQAL and SyAL is not independent of process corner variations.

Logic Designs	CSSAL[12]	SQAL[14]	SyAL[13]	WCS-QuAL

		1 MHz	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*
NOT/ BUF	FF	2.858	0.165	0.182	0.808	0.406	0.174	0.808	0.406	0.174	0.548	0.136	0.083
%NED		1.439	0.082	0.091	0.362	0.150	0.078	0.362	0.150	0.078	0.245	0.049	0.035
%NSD	SS	0.554	0.111	0.270	2.045	0.105	0.337	2.045	0.105	0.337	0.050	0.035	0.073
		0.271	0.055	0.118	0.857	0.047	0.177	0.857	0.047	0.177	0.022	0.019	0.030
AND/ NAND	FF	1.693	1.241	1.571	1.077	3.115	4.058	0.815	1.548	2.781	0.521	0.329	0.524
%NED		0.555	0.484	0.583	0.514	1.188	1.890	0.199	0.487	0.877	6.901	0.077	0.159
%NSD	SS	1.812	1.184	0.677	3.422	2.955	2.258	1.726	2.145	2.063	0.254	0.030	0.083
		0.641	0.350	0.307	1.215	0.924	1.043	0.534	0.609	0.505	0.074	0.007	0.028
OR/ NOR	FF	1.369	1.174	1.571	1.348	3.066	3.792	0.830	1.305	1.365	0.517	0.392	0.565
%NED		0.428	0.427	0.575	0.522	1.232	1.829	0.190	0.545	0.614	0.177	0.093	0.156
%NSD	SS	1.812	0.948	0.677	2.259	2.868	2.306	1.507	2.062	1.492	0.372	0.045	0.167
		0.641	0.339	0.307	0.957	1.030	1.029	0.488	0.673	0.471	0.109	0.001	0.052
XOR/ XNOR	FF	0.579	2.014	1.610	1.070	1.548	0.979	2.212	1.228	1.731	0.488	0.314	0.442
%NED		0.299	0.525	0.559	0.270	0.590	0.284	0.567	0.401	0.634	0.125	0.115	0.144
%NSD	SS	1.681	1.104	0.967	2.077	4.442	1.298	1.197	2.021	1.580	0.679	0.045	0.084
		0.810	0.359	0.333	0.479	1.119	0.312	0.444	0.591	0.596	0.163	0.011	0.043

TABLE III. PRE-LAYOUT SIMULATION RESULTS OF GATES AT FF AND SS CORNERS.

Fig 7 (a), (b), (c) and (d) shows the average energy dissipation per cycle of the AND/NAND gate at all five process corners at 1MHz, 10MHz and 100MHz for WCS-QuAL, CSSAL, SQAL, and SyAL respectively. Variations in process parameters can result in deviation of the device parameters from their nominal values. For instance, threshold voltage can vary for numerous reasons such as change in oxide thickness, substrate, implant impurity levels etc. The change in threshold voltage has impact on the Non Adiabatic Loss (NAL) in the adiabatic circuits and thus on the energy dissipation. Because WCS-QuAL QuAL completely removes the NAL from the evaluation phase, the average energy dissipation is less compared to the existing adiabatic secure logic at all process corners. This is an additional benefit of WCS-QuAL.

By contrast, CSSAL, SQAL, and SyAL show greater sensitivity to process corners especially at a higher frequency as can be seen from Fig. 7 (b), (c) and (d) respectively as they suffer from NAL during the evaluation phase. Also, the average energy dissipation increases significantly for CSSAL, SQAL, and SyAL as moving from 1MHz to 100MHz.

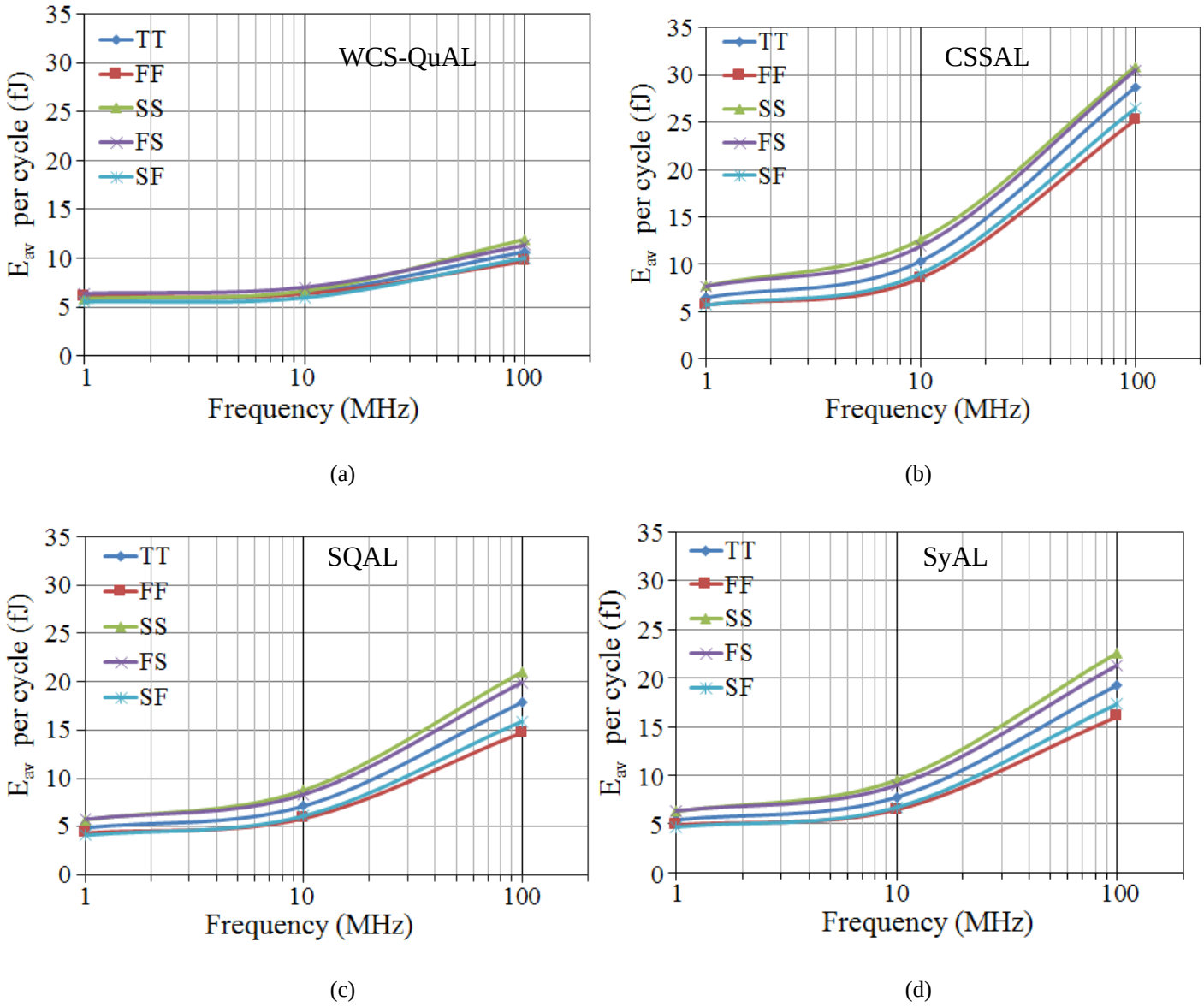


Fig. 7. Average energy dissipation per cycle under TT, FF, SS, FS and SF process corners (pre-layouts) of AND/NAND gate at 1MHz, 10MHz and 100MHz for (a) WCS-QuAL (b) CSSAL (c) SQAL and (d) SyAL.

6.4 Post-Layout Simulations

In order to get more realistic simulation results, full-custom layouts were drawn using Cadence Virtuoso™ layout editor. The post-layout simulations were carried out using the av-extracted file from the layout design with the resistance and capacitance (RC) parasitic parameters. The layouts for each of the logic gates using existing and WCS-QuAL were drawn and the simulations were performed for all five process corners. Fig 8 (a), (b), (c) and (d) shows the layout designs for NOT/BUF, AND/NAND, OR/NOR and

XOR/XNOR gates respectively using WCS-QuAL. The layouts for all the gates were drawn bearing in mind the need to maintain the symmetry and load balancing on the output nodes. The area is often sacrificed while maintaining the symmetry of the layouts.

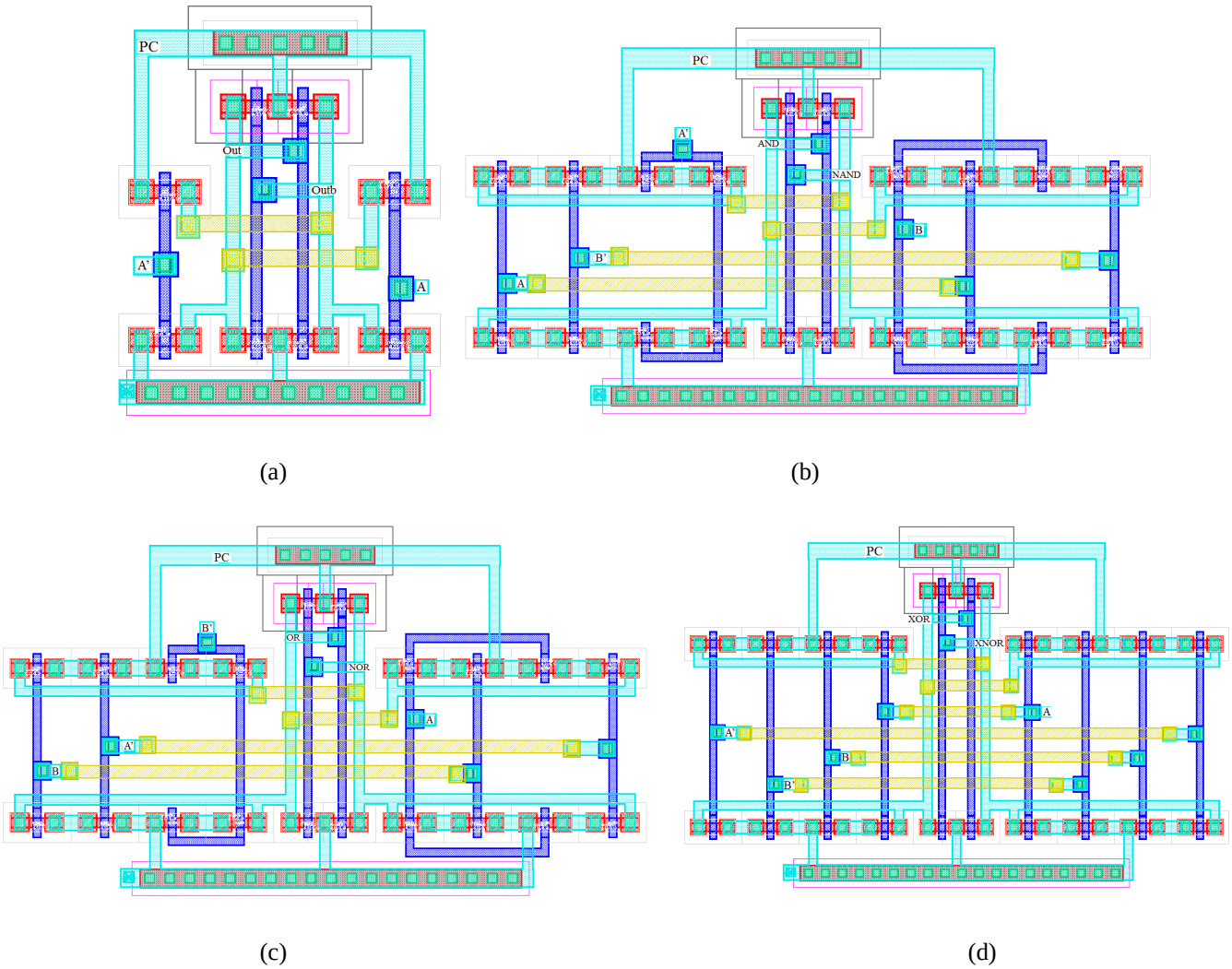


Fig. 8. Layout designs of WCS-QuAL (a) NOT/BUF (b) AND/NAND (c) OR/NOR (d) XOR/XNOR gates.

The numerical value of the layout area of the logic gates of the existing logic designs and WCS-QuAL is shown in Table IV. Due to the less number of transistors, SQAL exhibits the lowest layout area for all the logic gates. Except NOT/BUF gate using WCS-QuAL, all its 2-input gates consumes less area in comparison to the area consumed using CSSAL and SyAL. On the otherhand, CSSAL exhibits the highest layout area for all the logic gates.

Adiabatic Logic Gates	Layout Area (μm)^2			
	CSSAL	**SQAL**	**SyAL**	**WCS-QuAL**
NOT/BUF	6.68 x 7.97	6.28 x 5.42	6.28 x 5.42	6.44. x 7.13
AND/NAND	15.39 x 11.30	12.70 x 8.80	11.43 x 11.88	15.02 x 8.41
OR/NOR	15.39 x 11.30	12.70 x 8.80	11.43 x 11.88	15.02 x 8.41
XOR/XNOR	14.40 x 10.51	8.70 x 6.52	11.86 x 11.88	15.02 x 9.95

TABLE IV. LAYOUT AREA COMPARISON OF LOGIC GATES USING EXISTING AND WCS-QuAL

The post-layout simulation results are summarized in Table V. The results show that there is a significant difference in %NED and %NSD for WCS-QuAL and the existing secure adiabatic logic designs in comparison to their corresponding pre-layout simulation results. This significant difference is due to the complexity and difficulty of making layouts symmetric. Routing of charge sharing transistors and evaluation transistors makes the balancing of the two output nodes difficult which leads to higher values of %NED and %NSD. To improve the %NED and %NSD, routing of interconnects should be done carefully (equal lengths and widths of the complementary wires) such that the layouts are symmetric along X and Y axes. From Table V, the post-layout results confirm those repetition from the pre-layout simulations. The post-layout simulations of all the gates using WCS-QuAL, and existing logic designs at FF, SS, FS and SF process corners were also performed. They also show the similar trend as by the pre-layout simulation results but having higher values of %NED and %NSD.

Logic Designs	**CSSAL[12]**	**SQAL[14]**	**SyAL[13]**	**WCS-QuAL**

	1 MHz	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*	*1 MHz*	*10 MHz*	*100 MHz*
NOTBUF												
%NED	8.804	6.760	5.690	7.873	6.775	3.624	7.873	6.775	3.624	2.505	2.080	1.202
%NSD	5.316	3.990	3.310	4.376	3.367	2.092	4.376	3.367	2.092	1.310	1.017	0.439
AND/NAND												
%NED	13.18	13.910	12.450	14.97	14.37	13.840	14.02	13.760	13.230	7.483	8.099	7.106
%NSD	5.120	6.060	5.660	5.813	6.507	6.226	6.487	6.273	5.422	2.281	3.416	2.851
OR/NOR												
%NED	13.64	13.740	12.740	14.66	14.45	13.84	14.09	12.956	13.185	7.888	7.656	6.555
%NSD	5.400	6.170	5.860	6.320	6.019	6.299	6.822	6.645	5.715	3.718	3.352	2.738
XOR/XNOR												
%NED	10.65	11.86	9.515	9.360	4.023	8.469	10.78	11.472	9.851	6.431	7.461	4.397
%NSD	4.130	5.200	4.010	2.741	1.441	2.779	4.970	3.770	4.116	2.405	2.974	1.606

TABLE V. POST-LAYOUT SIMULATION RESULTS OF GATES USING WCS-QuAL AND EXISTING LOGIC

6.5 Case Study:8-bit Montgomery Multiplier

The Montgomery multiplier plays an important part in the field of cryptography. It is the basic building block of public key cryptography algorithms such as Rivest-Shamir-Adleman (RSA) cryptography Algorithm [19] and the Elliptic Curve Cryptography (ECC) algorithm [20]. To evaluate the performance of WCS-QuAL an 8-bit Montgomery multiplier was implemented. For comparison, CSSAL, SQAL and SyAL logic versions were also implemented. 8-bit Montgomery multipliers were implemented using systolic array architecture. For an 8-bit Montgomery Multiplier, eight residue computation units are required. Each residue computation unit is made of many Processing Elements (PEs), AND/NAND, XOR/XNOR, synchronization NOT/BUF and resettable NOT/BUF gates which work in a cascade manner to calculate the residue from that unit. The PEs in the architecture comprises of either half adders or full adders.

6.5.1 Impact of the number of inputs in the secure adiabatic logic designs

In a full adder, with 3 inputs it becomes difficult to balance the output nodes not only because of a large number of transistors (for balancing) but also because many are stacked. Thus, full adders for the

Montgomery multiplier were implemented using three cascaded stages of logic gates using WCS-QuAL and existing logic. This way, the full adder which in a normal adiabatic logic would require only one phase of the power-clock, it required 3 phases to deliver the sum and the carry outputs using secure adiabatic logic thus, increasing the latency and decreasing the throughput.

6.5.2 Impact of frequency on NED, NSD and average energy

Simulations for the Montgomery multipliers were performed at 1MHz, 13.56MHz and 100MHz frequencies and 10fF load capacitance. The energy dissipation is measured per cycle for 10 random input patterns. The simulation results for the existing and WCS-QuAL are summarized in Table VI.

WCS-QuAL exhibits the lowest value of %NED and %NSD for the simulated frequencies. The ranking of performance (based on %NED and %NSD) changes for existing logic at simulated frequencies. At 1MHz and 100MHz, CSSAL is second best followed by the SyAL and SQAL, whereas, at 13.56MHz, SyAL is second best and is followed by CSSAL and SQAL.

Designs	**CSSAL[12]**			**SQAL[14]**			**SyAL[13]**			**WCS-QuAL**		
	1 MHz	***13.56 MHz***	***100 MHz***	***1 MHz***	***13.56 MHz***	***100 MHz***	***1 MHz***	***13.56 MHz***	***100 MHz***	***1 MHz***	***13.56 MHz***	***100 MHz***
%NED	1.728	2.829	2.475	3.646	3.453	3.835	2.113	1.828	2.894	0.725	0.749	0.673
%NSD	0.693	0.805	0.795	0.947	0.666	1.390	0.592	0.664	0.801	0.205	0.254	0.189

TABLE VI. PRE-LAYOUT SIMULATION RESULTS COMPARING THE %NED AND %NSD OF 8-BIT MONTGOMERY MULTIPLIER USING WCS-QuAL AND EXISTING LOGIC.

Fig.9 shows the graph of average energy dissipated per cycle by WCS-QuAL, CSSAL, SyAL and SQAL across the selected frequency range. As expected from gate level simulation results, WCS-QuAL exhibits the minimum energy dissipation at frequencies above 20MHz. It can be seen that at low frequencies (~1MHz) the four logic families show broadly similar energy consumption with SQAL consuming around 20% less than the others. However, as operating frequency increases, Adiabatic losses start to become

significant albeit less so in the case of the WCS-QuAL because of the low ON-resistance (due to the formation of transmission gate pair N3, P1 and N4, P2 in Figure 3(a)), which at 100MHz dissipates least energy. CSSAL consumes the maximum energy at all simulated frequencies. As the frequency of operation is increased, the Adiabatic Losses (AL) increases. The AL combined with NAL in SQAL, SyAL and CSSAL makes the energy dissipation worst in comparison to WCS-QuAL.

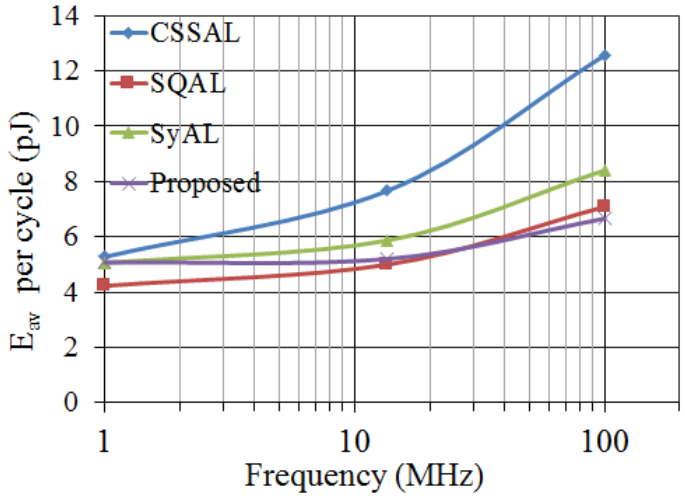


Fig. 9. Average energy per cycle measured from pre-layout simulations of 8-bit Montgomery Multiplier for CSSAL, SQAL, SyAL, and WCS-QuAL at frequencies ranging from 1MHz to 100MHz.

6.5.3 Impact of power supply scaling

Since one of the dominant components of the energy dissipation in adiabatic logic is supply voltage, energy can be reduced by reducing the power supply. Reduction in supply voltage affects the gate overdrive voltage, V_{GS}-$V_{th,}$ and on-resistance of the transistors in the charging path. With the reduction in supply voltage, an increase in on-resistance is observed [22]. Therefore, it is important to evaluate the impact of power-clock scaling on the performance of the secure adiabatic logic designs.

The power-clock was scaled from 1.8V down to 0.6V. The simulation results are summarized in Table VII. Since the simulation results for 1.8V power supply were included in Table VI, they are omitted in Table VII. As SQAL and SyAL logic doesn't have cross-coupled nMOS transistors in the latch thus, they

suffer from coupling effect causing one of the output node to be coupled to the other output node following the power-clock. As a result, the zero logic in SQAL and SyAL stays at around 200mV causing functionality failure below 0.6V.

WCS-QuAL, on the other hand, uses dual evaluation network one connected between the power-clock and the output node and the other connected between the output node and ground. It also has cross-coupled nMOS transistors in the latch and thus, its logic zero remains close to zero. The comparison between secure adiabatic logic designs in terms of average energy, %NED and %NSD is tabulated in Table VII

Logic Designs	**Power-clock scaling @ 13.56MHz**				
	V=.6	**V=.8**	**V=1**	**V=1.2**	**V=1.5**
CSSAL					
E_{av}(pJ)	1.322	2.803	3.553	4.243	5.249
%NED	1.320	1.732	1.703	1.683	1.209
%NSD	0.342	0.707	0.680	0.716	0.338
SyAL					
E_{av}(pJ)	1.205	2.171	2.619	3.210	4.236
%NED	1.809	1.417	1.666	1.790	1.731
%NSD	0.962	0.752	0.885	0.952	0.920
SQAL					
E_{av}(pJ)	0.999	1.770	2.258	2.786	3.609
%NED	2.941	2.793	2.451	3.169	3.493
%NSD	1.251	1.205	1.224	1.665	1.483
WCS-QuAL					
E_{av} (pJ)	1.297	1.617	2.016	2.637	3.681
%NED	0.643	0.678	0.691	0.793	0.622
%NSD	0.196	0.309	0.304	0.373	0.329

TABLE VII. PRE-LAYOUT SIMULATION RESULTS COMPARING PERFORMANCE OF MONTGOMERY MULTIPLIER AGAINST POWER SUPPLY SCALING

Fig. 10 illustrate the relationship between %NED and power-clock scaling for WCS-QuAL and the existing secure logic. The proposed logic shows the least values of %NED followed by CSSAL, SyAL and SQAL.

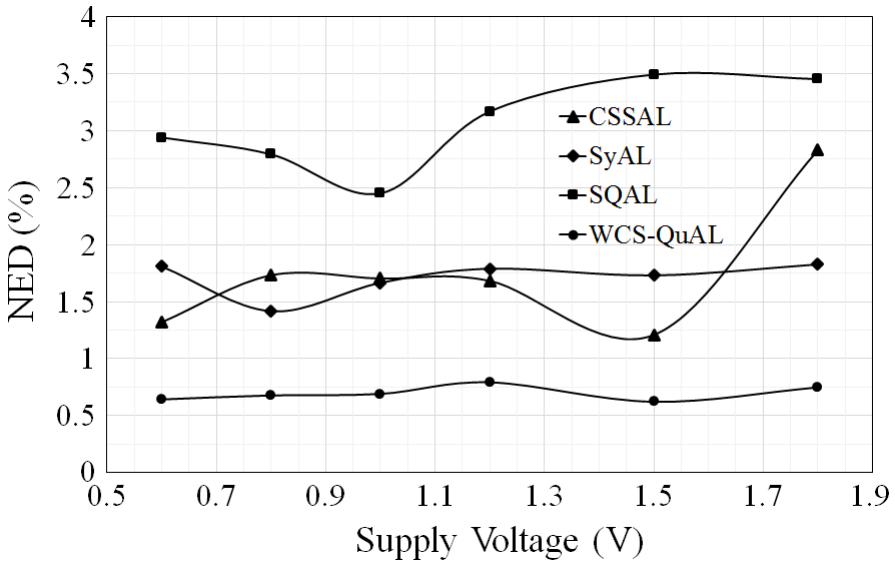


Fig. 10. %NED vs supply voltage at 10MHz.

6.5.4 Comparison of the proposed and the existing logic designs on the basis of voltage sources required and transitor counts.

Table VIII compares WCS-QuAL and existing logic on the basis of the number of voltage sources required and the number of transistors used in the implementation of 8-bit Montgomery Multiplier. Because WCS-QuAL works on 4-phase power-clocking scheme in cascade stages, 8-bit Montgomery multiplier design using WCS-QuAL requires four voltage sources. On the other hand, SQAL and SyAL also work on 4-phase power-clocking scheme and use charge sharing input therefore, requiring four voltage sources each for 4-phases of the power-clocks and for generating 4-phases of the charge sharing input. In total, eight voltage sources are required. In [14] the authors omitted, four voltage sources used for generating the 4-phases of the charge sharing inputs in the results. Similarly, CSSAL works on 4-phase power-clocking scheme requiring four voltage sources. Additionally, it uses charge sharing and evaluation input, therefore four phases of each charge-sharing and evaluation inputs need to be generated which requires additional eight voltage sources. In total, twelve voltage sources are required in the design using CSSAL.

Although for the design of the 8-bit Montgomery multiplier, WCS-QuAL uses highest number of transistors (≈36,000) which is 75.6%, 34.8% and 4% more transistors in comparison to SQAL, SyAL, and CSSAL respectively, it consumes the lowest energy at frequencies ranging from 20MHz to 100MHz. Its higher energy disspation is due to the higher leakage current dominant at lower frequency.

Logic	Required number of voltage sources	Number of logic gates in Montgomery Multiplier		Number of transistors per gate	Total number of transistors (Approx.)
WCS-QuAL	4	NOT/BUF	297	8	36,336
		AND/NAND	734	20	
		OR/NOR	49	20	
		XOR/XNOR	716	20	
		Reset BUF	199	20	
SQAL[17]	8	NOT/BUF	297	5	20,695
		AND/NAND	734	13	
		OR/NOR	49	13	
		XOR/XNOR	716	9	
		Reset BUF	199	13	
SyAL[16]	8	NOT/BUF	297	5	26,955
		AND/NAND	734	15	
		OR/NOR	49	15	
		XOR/XNOR	716	15	
		Reset BUF	199	15	
CSSAL[12]-[15]	12	NOT/BUF	297	9	34,935
		AND/NAND	734	19	
		OR/NOR	49	19	
		XOR/XNOR	716	19	
		Reset BUF	199	19	

TABLE VIII. COMPARISON OF REQUIRED VOLTAGE SOURCES AND TRANSISTOR COUNTS OF WCS-QuAL AND THE EXISTING LOGIC.

7. CONCLUSION

In this paper, we present WCS-QuAL adiabatic logic which doesn't require any charge-sharing between the output/internal nodes of the gate as a countermeasure against power analysis attacks. During the evaluation phase of the power-clock, WCS-QuAL suffers from zero NAL. The pre-layout and post-layout simulation results show that WCS-QuAL outperforms the existing secure adiabatic logic at all process corners at all simulated frequencies and shows the least sensitivity to process corners. In addition, all the 2-input gates using WCS-QuAL consume nearly equal energy. These results were confirmed by implementing an 8-bit Montgomery multiplier as a candidate circuit for comparison. Simulation results show that WCS-

QuAL exhibits the least (i.e. best) value of NED and NSD against frequency variations and power supply scaling.

Acknowledgement

The authors wish to thank the University of Westminster for awarding Cavendish Research Scholarship for carrying out the research in the Department of Engineering. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

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, Lecture Notes In Computer Science, pp. 388–397, 1999.

[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, DOI: 10.1109/MDT.2007.200.

[3] 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, pp. 403–406, 2002.

[4] T. S Messerges, E. A Dabbish, and R. H Sloan, " Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002, DOI: 10.1109/TC.2002.1004593.

[5] T. Popp and S. Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints", in Proc. CHES, Edinburgh, UK, pp. 172–186, 2005, DOI: 10.1007/11545262_13.

[6] Z. Chen and Y. Zhou, "Dual-rail random switching logic: A countermeasure to reduce side channel leakage", in Proc. CHES, Yokohama, Japan, pp. 242–254, 2006, DOI: 10.1007/11894063_20.

[7] S. Mangard, T. Popp, and B. Gammel, "Side-Channel Leakage of Masked CMOS Gates", in Proc. CT-RSA, San Francisco, CA, USA, pp. 351–365, 2000, DOI: 10.1007/978-3-540-30574-3_24.

[8] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", in *Proc. ESSCIRC*, Paris, pp. 246–251, 2004, DOI: 10.1109/DATE.2004.1268856 .

[9] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style", in Proc. CHES, pp. 255–269, 2006, DOI: 10.1007/11894063_21 .

[10] M. Bucci, L. Giancane, R.o Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Precharge Logic", In proc. CHES 2006, LCNS, vol. 4249, pp. 232–241, 2006, DOI: 10.1007/11894063_19.

[11] W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis and E. Ying-Chin Chou, "Low-Power Digital Systems Based on Adiabatic switching Principles", IEEE Transactions on VLSI Systems, Vol. 2, No. 4, pp. 398–407, 1994, DOI: 10.1109/92.335009 .

[12] C. Monteiro, Y. Takahashi, and T. Sekine, "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level", Microelectronics Journal, vol 44, no. 6, pp. 496–503, 2013, DOI:10.1016/j.mejo.2013.04.003.

[13] 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, http://dx.doi.org/10.4218/etrij.10.0209.0247.

[14] 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, DOI: 10.1109/TCSI.2014.2359720.

[15] Y. Moon, and D.K. Jeong, "An efficient charge recovery logic circuit", IEEE J. Solid-State Circuits, vol. 31, no. 4, pp. 514–522, 1996, DOI: 10.1109/4.499727.

[16] 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, DOI: 10.1109/9780470544846.ch3.

[17] F. Mac´e, F.-X. Standaert, J.-J. Quisquater, " Information Theoretic Evaluation of Side-Channel Resistant Logic Styles", in Proc. CHES, LNCS, vol 4727, pp 427–442, Vienna, 2007, DOI: 10.1007/978-3-540-74735-2_29.

[18] K. Tiri, “Side-channel attack pitfalls”, ACM/IEEE DAC, pp. 15–20, 2007.

[19] R. L. Rivest, A. Shamir, and L. Adleman “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, vol.21, no. 2, pp.120–126, 1978, DOI<10.1145/359340.359342.

[20] N. Koblitz, “Elliptic curve cryptosystems”, Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987, DOI: https://doi.org/10.1090/S0025-5718-1987-0866109-5.

[21] J. Fisher, E. Amirante, F. Randazzo, G. Inannaccone, D. Schmitt-Landsiedel, “ Reduction of the Energy Consumption in the Adiabatic Gates by Optimal Transistor Sizing”, in *Proc.* PATMOS, pp. 309–318, 2003, DOI: 10.1007/978-3-540-39762-5_37.

[22] P. Teichmann, “Adiabatic logic: future trend and system level perspective”, vol. 34. Springer Science & Business Media, 2011, DOI: 10.1007/978-94-007-2345-0.

[23] S. Nakata, H. Makino, J. Hosokawa, T. Yoshimura, S. Iwade, Y. Matsuda, “Energy Efficient Stepwise Charging of a Capacitor Using a DC-DC Converter With Consecutive Changes of its Duty Ratio,” IEEE Transactions on Circuits and Systems I, vol. 61, no. 7, pp. 2194-2203, 2014.

[24] E. Tena-Sánchez, 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, 2014, DOI: 10.1109/JETCAS.2014.2315878.

[25] L. Lin and W. Burleson, “Analysis and Mitigation of Process Variation Impacts on Power-Attack Tolerance”, in *Proc.* DAC, pp. 238 – 243, San Francisco, 2009.

[26] C. Monteiro, Y. Takahashi, and T. Sekine, “Effectiveness of Dual-Rail CSSAL against Power Analysis Attack under CMOS Process Variation”, in *Proc.* APCCAS, pp. 121–124, Ishigaki, 2014, DOI: 10.1109/APCCAS.2014.7032734.