Effects of logic glitch and (area-power dissipation) leakage on cryptosystems using clock gating technique to enhance web etiquette

Akhigbe-mudu Thursday Ehis[1]

[1] Department of Computer Science, Faculty of Applied Sciences and Engineering, African Institute of Science Administration and Commercial Studies Lome, Republic du Togo

Correspondence: Akhigbe-mudu Thursday Ehis, Department of Computer Science, Faculty of Applied Sciences and Engineering, African Institute of Science Administration and Commercial Studies Lome, Republic du Togo. E-mail: akhigbe-mudut@iaec-university.tg

Received: April 05, 2023 Accepted: June 29, 2023 Published: December 01, 2023

DOI: 10.14295/bjs.v2i12.364 URL: https://doi.org/10.14295/bjs.v2i12.364

Abstract

The last century has seen an evolution in technology that has improved communication systems and, in general, made life easier for people. Our communication systems have become faster and more dependable as a result of the explosion of gadgets and services. But, these upgrades come at a price. The power consumption is one of the most worrying costs. In recent years, the solution involved installing larger, more powerful batteries—so long as doing so did not limit mobility. Today's economic and environmental problems compel us to consider alternative solutions, like methods for lowering the power consumption of digital devices. This study focuses on using digital circuits, which promise to deliver good energy efficiency and desirable performance at very low voltage savings. Certain digital switches are allegedly redundant and not required for the circuit to function properly, yet they continue to use energy. So, one of the primary issues for low power design is reducing such redundant switches. Subthreshold conduction in digital circuits is typically seen as a "parasitic" leakage in a condition where there should ideally be no conduction. Sub-threshold activities thereby reduce the problem of lowering power consumption, but do so at the expense of system throughput deterioration, fluctuations in system stability and functionality, temperature variations, and most critically, design space utilization. In order to minimize some of these redundant switches and to make circuits more energy-efficient while maintaining functionality, this study suggests two novel techniques. It uses an optimization method based on threshold voltage change to reduce glitch power. A glitch-free circuit netlist is created using an algorithm, while still maintaining the requisite delay performance. Using this approach results in a 6.14% overall reduction in energy consumption.

Keywords: clock-gating, leakages, logic glitches, power dissipation, sub-threshold leakages

Efeitos da falha lógica e fuga (dissipação de energia de área) em sistemas criptográficos usando a técnica de *clock gating* para aprimorar o protocolo na web

Resumo

O último século assistiu a uma evolução da tecnologia que melhorou os sistemas de comunicação e, em geral, facilitou a vida das pessoas. Nossos sistemas de comunicação tornaram-se mais rápidos e confiáveis como resultado da explosão de aparelhos e serviços. Mas, essas atualizações têm um preço. O consumo de energia é um dos custos mais preocupantes. Nos últimos anos, a solução envolveu a instalação de baterias maiores e mais potentes, desde que isso não limitasse a mobilidade. Os problemas econômicos e ambientais de hoje nos obrigam a considerar soluções alternativas, como métodos para reduzir o consumo de energia de dispositivos digitais. Este estudo se concentra no uso de circuitos digitais, que prometem oferecer boa eficiência energética e desempenho desejável com economia de tensão muito baixa. Certos interruptores digitais são supostamente redundantes e não são necessários para o funcionamento adequado do circuito, mas continuam a consumir energia. Portanto, um dos principais problemas para o projeto de baixo consumo de energia é reduzir esses *switches* redundantes. A condução abaixo do limiar em circuitos digitais é normalmente vista como uma fuga “parasita” em uma condição em que idealmente não deveria haver condução. As atividades abaixo do limite reduzem, assim, o problema de diminuir o consumo de energia, mas o fazem às custas da deterioração da taxa de transferência do sistema, flutuações na estabilidade e funcionalidade do sistema, variações de temperatura e, mais criticamente, utilização do espaço de projeto. A fim de minimizar alguns desses *switches* redundantes e tornar os circuitos mais eficientes em termos de energia, mantendo a funcionalidade, este estudo sugere duas novas técnicas. Ele usa um método de otimização baseado na mudança de tensão limite para reduzir a energia de falha. Uma *netlist* de circuito sem falhas é criada usando um algoritmo, mantendo o desempenho de atraso necessário. O uso dessa abordagem resulta em uma redução geral de 6,14% no consumo de energia.

Palavras-chave: *clock-gating*, fugas, falhas lógicas, dissipação de energia, fugas abaixo do limite.

1. Introduction

Technology has advanced over the past century to offer improved communication systems that, in general, make life simpler for the human population. Our communication systems have gotten faster and more dependable as a result of the explosion of gadgets and services that have emerged in recent decades. This was only made possible by the advancements in compute power, speed, and reliability of communications as well as the increased power of mobile electronic devices.

Nevertheless, each development came at a price. The power consumption is one of the most worrying costs. In recent years, the solution was to place larger, more powerful batteries, as long as doing so did not limit mobility. Economic and environmental challenges in the present day urge us to consider alternative solutions, such as methods of reducing the power consumption of digital devices (Gabriel et al., 2022).

The goal of this study is to decrease dynamic power consumption in integrated circuits, or the power lost when transistors are charged or discharged when logical gates in the circuit change their values. Although some of these switches are frequently redundant and don't need to be present for the circuit to function properly, they nevertheless use energy. Reducing such redundant switches is thus one of the main challenges for low power design. Two distinct methods were created to reduce some of these superfluous switches and increase the energy efficiency of circuits without sacrificing functionality (Zaynab et al., 2022).

Network routers of today must handle enormous traffic levels without degrading performance. Since sensor nodes are commonly put in locations with little protection and may be vulnerable to hostile attackers, security in wireless sensor networks is essential. One node may be taken by malicious attackers, but the overall effect could be quite harmful. Here are a few instances of relatively limited applications that demand the development of efficient and low-energy security mechanisms. Symmetric key cryptography may not be the ideal choice for security-restricted applications where keeping symmetric keys poses a risk, such as RFID tags or sensor nodes, according to recent literature. Furthermore, to the overhead for their side channel information attack defenses.

Because to its benefits over conventional systems, elliptic curves cryptography, (ECC) has lately gained popularity in a number of applications. It is a well-known public key cryptography system that provides a greater level of security than RSA scheme, making it significantly superior to RSA cryptography (Mainu & Matei, 2022).

1.1. How does ECC Function

But how exactly does the underlying Trapdoor Function work, and what is an elliptic curve? An elliptic curve is a set of points that satisfy a specific mathematical equation. This is how an elliptic curve's equation looks, and it is visualized graphically in figure 1 below:

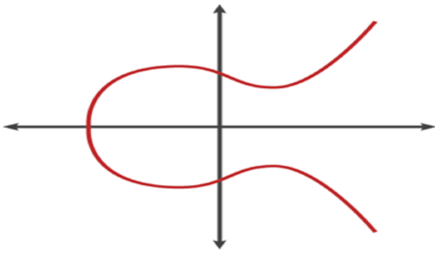


Figure 1. Elliptic Curve Trapdoor Function. Source: Author, 2023.

It is possible to multiply a point on a curve by a number to get another point on the curve, but even if you know the starting point and the result, it could be difficult to figure out what number was used. For cryptographic applications, elliptic curve-based equations have the advantage of being both extremely challenging to reverse and relatively easy to perform. Hence, for numbers of the same size, factoring is substantially simpler than computing discrete elliptic curve logarithms (Oguz & Mehmet, 2022). Because a harder, more computationally expensive challenge necessitates a more durable cryptographic strategy, elliptic curve cryptosystems are more difficult to break than RSA and Diffie-Hellman (Danquah et al., 2020).

1.2. Logic Glitches

The switching activity in the circuits are a significant role in the power consumption of CMOS combinational logic circuits. Glitches, or erroneous pulses, are the cause of many of these switching actions. But think about what occurs in case the signal A goes from 1 to 0, as shown in figure 2. A bug is used to describe this bogus 0. It is a good idea to design circuits that are insensitive to glitches because these errors may or may not have disastrous consequences (Wuchan & Oiwen 2022)

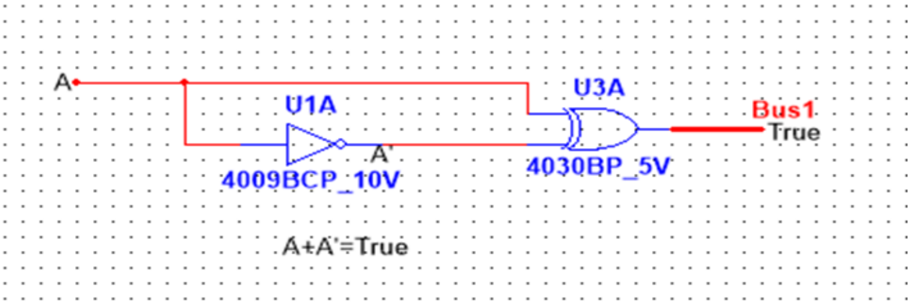


Figure 2. Depicted Logic Glitch. $\boldsymbol{i.e.A+\bar{A}=True}$. Source: Author, 2023.

Propagation delays not only restrict the speed at which a circuit may work, but they can also cause unexpected and unwanted transitions in outputs. These unwanted transitions, sometimes known as "glitches," happen when an input signal changes states, provided the signal travels along two or more paths through a circuit and one of those paths has a longer delay than the others. The larger delay on one path can cause a glitch when the signal channels are recombined at an output gate. Asymmetric path delays typically happen when an input signal travels along two or more pathways, one of which has an inverter and the other does not. Figure 3 below displays a malfunction brought on by an inverter. Note the error (the 1-0-1 transition on Y) has the same duration as the delay in the inverter (Faheem et al., 2022).

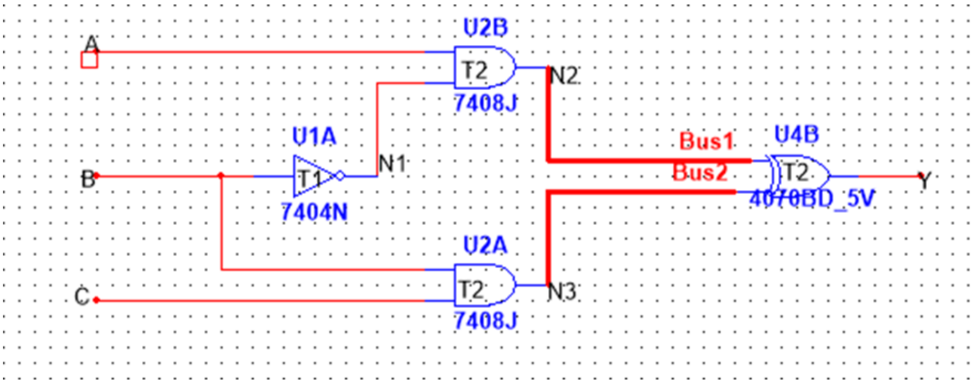


Figure 3. Glitch Logic Circuit. Source: Author, 2023.

The amount of delay added to logic signals by all logic gates depends on how they are built and how much output loading they have (Shanthi et al., 2018). The inverter is depicted in Fig. 3 with a longer delay (denoted by time T1) than the other gates (T2). This fabricated example shows the overly lengthy inverter delay's part in producing an output glitch, yet a glitch would still arise regardless of the delay time. It is evident from the timing diagram how the inverter delay is connected to the output glitch (Sun & Tian, 2022).

1.3. Leakage of Currents

Transistors are not perfect switches – they always "leak", Especially the high performance (low Vth) ones- (Figure 4).

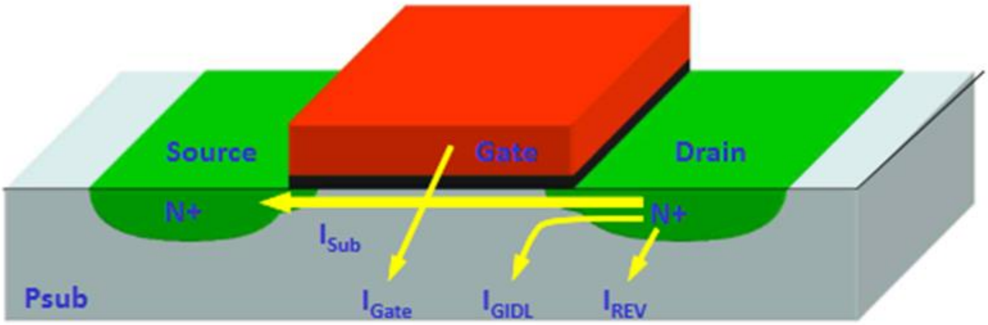


Figure 4. Total leakage Current. Source: Author, 2023.

$$TotalLeakage = I_{sub} + I_{gate} + I_{GIDL} + I_{rev} \qquad (1)$$

I_{sub}: Sub-threshold Leakage

I_{gate}: Gate oxide Leakage

I_{GIDL}: Gate Induce Drain Leakage

I_{rev}: Reverse Bias Junction Leak

However, gate leakage is becoming significant, and can be mitigated.

1.4. Subthreshold leakage Isub

Leakage between Drain and Source when (Figure 5).

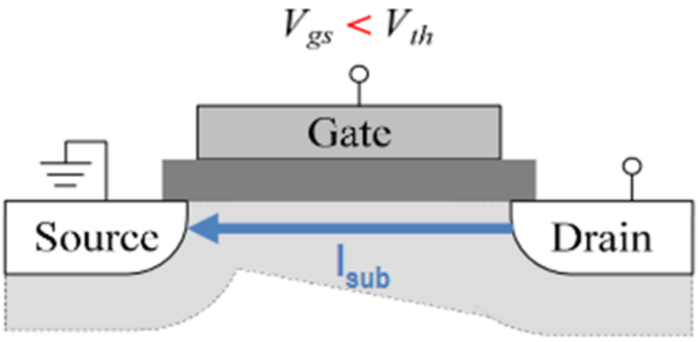


Figure 5. Leakage between Drain and Source. Source: Author, 2023.

1.5. Oxide Leakage

Tunneling effect

- Electromagnetic wave strike at barrier;
- Reflection + Intrusion into barrier;
- If thickness is small enough;
- Wave interfuse barrier partially (Figure 6).

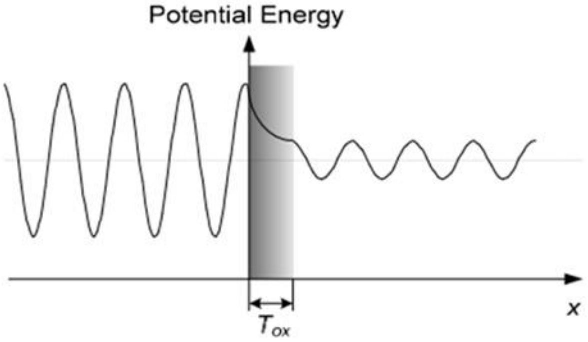


Figure 6. Gate Oxide Leakage. Source: Author, 2023

1.6 Oxide leakage Igate (Tunneling Effect)

- In Nanometer-Transistors, where Tox < 2 nm;
- Electrons tunnel through gate oxide;
- Leakage current (Figure 7).

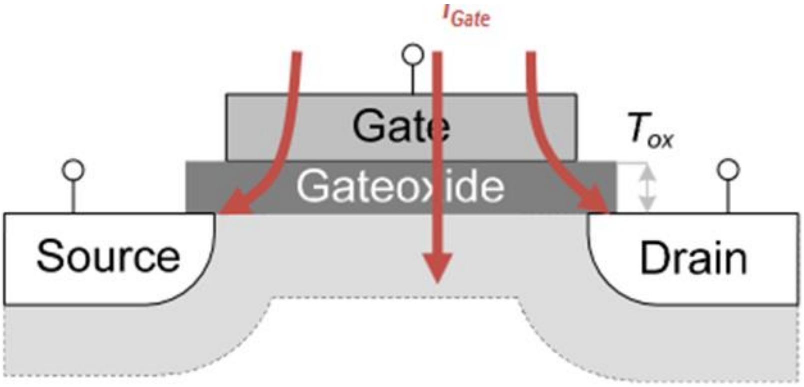


Figure 7. Gate Oxide Leakage. Source: Author, 2023.

1.7. Statement of the Problem

This study focuses on using digital circuits, which promise to deliver excellent energy savings and desirable performance at very low voltage. Energy usage must be effectively very low in industries like bioengineering and smart sensors to ensure long battery life. This is made possible by the sensors' use of energy-harvesting strategies from the environment in which they are placed. The need for power optimization that makes use of sub-threshold circuits techniques is pushed by the need to employ the energy harvester economically and reliably manage the performance of the drive system at very low supply voltages (Lara-Nino et al., 2019).

In digital circuits, subthreshold conduction is frequently viewed as a parasitic leakage in a situation where there should ideally be no conduction. Sub-threshold operations therefore reduce the issue of increasing power consumption, but they do so at the expense of decreased system throughput, changes in system functioning and stability as a result of process and temperature variations, and most critically, reduced design area utilization.

Lower power consumption is crucial for longer battery life in today's semiconductor designs for mobile and portable applications (Sunglin et al., 2022). Power consumption has been a major concern for usability and reliability difficulties with semiconductor goods as a result of the rise in popularity of portable devices like smartphones in recent years. This is due to the linear relationship between power and voltage and the frequency of the clock, as seen by the equation below: (2)

One of the key factors influencing how much power is utilized in CMOS combinational logic circuits is the switching activity in the circuits. These switching behaviors are frequently caused by spurious pulses, also referred to as glitches. Recent years have seen a rise in the number of portable devices, such as smartphones, and as a result, power consumption has become a major concern for usability and reliability difficulties with semiconductor products. Thus, it's important to reduce clock power. Clock gating is a vital power-saving technique that is frequently applied using tools for gate-level power synthesis (Anyanwu et al., 2023).

This article discusses the use of clock gating techniques to save power consumption and emphasizes how clock gating impacts a number of design procedures, including testability and metastability with clock domain crossings. The article also details the do's and don'ts of clock gating to avoid chip failures and unnecessary power dissipation.

1.8 Related Work

Integer-factorization methods served as the basis for the Public Key Encryption Techniques and Algorithms that evolved from Rivest, Shamir, and Adleman (RSA) (Diana & Alexandra 2022). Key exchange was based on Diffie-Hellman, the Digital Signature Algorithm (DSA), which uses Elgamal encryption, or Discrete Logarithm Schemes. Elliptic curve key exchange (ECDH) based on elliptic curve techniques and elliptic curve digital signature algorithms can offer levels of security with short keys. With the aid of public key systems, services like digital signature, non-repudiation, digital certificate, and confidentiality can be provided (Shah et al., 2022).

Clock gating is a widely used method that dynamically switches the clock network, which often accounts for 30–40% of the total power consumption of a modern LSI design. This method reduces power dissipation while only incurring a minimal area and time penalty (Jisha & Speaka, 2019). The majority of existing clock gating techniques (Petru & Floin, 2022) rely on manually locating architectural components that can be disabled utilizing data from the current and subsequent state functions of a register. They must, however, navigate a vast stage area, especially when numerous registers need to be gated simultaneously. The additional external control circuitry raises the power and area requirements of the initial design.

The outcomes of the method's application are illustrated by (George et al., 1998) by converting a number of ISCAS89 combinational circuits to sequential circuits. The clock gating logic's power estimates, which takes switching activity into account, deviates from the original approach and seems to underestimate the results of our tests. (Petru & Leon, 2022) introduces numerous clock gating option combinations using a commercial tool. Yet, they make no optimization recommendations. Recent studies have proposed a candidate extraction and control signal selection-based automatic clock gating technology and optimization method (Karim et al., 2021). Compared to conventional procedures, this one utilizes less energy. The most fundamental form of control in a digital circuit is the clock signal.

The fundamental principle of clock design for a very long time was that the signal should be kept as pure as possible and that a circuit designer shouldn't interrupt or deactivate a clock signal. It has only recently been discovered that the clock signal is a substantial source of power consumption due to the additional activity it produces in the underlying logic modules (Anyanwu et al., 2022).

The push was made to gate the clock signal and disable some of the clock tree distribution in order to decrease power dissipation (Gaupa & Akhter, 2022). The comprehensive overview of clock dissemination mechanisms can be found in (Pakkiraiah & Satyanarayana, 2022). While introducing clock gating can greatly increase a design's power efficiency, doing so makes it more difficult to disperse the clock signal.

Although gated groups are created from the circuit's logical model, gating at the logic level ignores the physical layout and placement of the group members. To get at the best outcome, an efficient low power gated clock tree tool must strike a compromise between logical and physical design elements (Sghaler et al., 2022).

2. Materials and Methods

2.1 Dissipation of Power Model

The dynamic power dissipation of a CMOS gate can be calculated by:

$$P_{gate} = \frac{1}{2}\sum_{x_i gate.input} C_{xi} V^2 f E(x_i) \qquad (1)$$

Where V is the supply voltage, f is the clock frequency, $C_{x_i}$is the gate capacitance of the $i-th$ input and $E(x_i)$ is the transition probability of the i^{th} input signal. A input signal, x_i of a logic circuit can be described accurately with two statistical attributes, namely the static probability $P(x_i)$ and transitional probability$E(x_i)$.

Definition1: the static probability, $P(x_i)$ of the signal x_i is defined as the percentage of the clock cycle in which the signal is in high logic level.

Definition 2: The transition probability, $E(x_i)$ of a signal $x_i$is defined as the probability a transition to occur either from logic value one to zero or from logic value zero to one, during two successive clock cycles.

Adopting the power model proposed in [9], it is assumed that the primary inputs are mutually independent and each primary input is fist order temporally dependent. Given a logic function, $F = f(\underline{x}) = f(x_0, x_1, ---, x_{n-1})$, the associated transition function $(Tf)$is defined as:

$$Tf = f(\underline{x}^0) \oplus f(\underline{x}^T) \qquad (2)$$

Where $f(\underline{x}^0)$ and $f(\underline{x}^T)$ are values of the function at time instances $t = 0..andt = T, respectively.$ Studying eqn (2) we infer that the transition function depends on the primary inputs and takes the value one, iff a transition occurs between two successive clock cycles. Therefore, the Required Transition Probability $E(F)$, of the function F can be calculated as$E(F) = P(Tf = 1)$. We deal with logic function implemented by two-level circuits, where the first level consists of AND gates and the second one consists of an OR gate. In general, an AND gate makes an output transition, if at least one primary input changes its logical state $(i.e1 \to 0, 0 \to 1)$within two successive cycles, while the remaining inputs are in the logic state one. All the possible input combinations of an n-input AND gate, which cause an output transition can be calculated by:

$$\binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n - 1,$$

Where $\binom{n}{x}$ means that x signals perform simultaneously the same transition $(1 \to 0, 0 \to 1)$

Adopting the fundamental principles of [9], the transition probability of an n-input, AND gate (a similar form for an A-input OR gate), $f = (x_0, x_1, \ldots, x_{n-1}), can.be.exp\,r\,essed.as$:

$$E(F) = 2\sum_{j=0}^{2^n-2} \coprod_{i=0}^{n-1} \{b_i(j) p_{11}(x_i) + (1 - b_i)(j)(p_{10}(x_i)\} \qquad (3)$$

Where $b_i(j) \in (0,1)$ is the value of thei^{th},$i = 0,1, \ldots, n-1$ bit of thej^{th},$j = 0,1 \ldots 2^n - 2$ input combination. Also $P_{11}(x_i)..and..P_{10}(x_i)$ are the probability of the input signal x_i to make the transition $(1 \to 1, and. 1 \to 0)$within two successive clock cycles respectively. Equation (3) is used to calculated the E(F) in place of Reduced Ordered Binary Decision diagrams (RBDD). Also the term 2 of equation (3) arises from the fact that:

$$P_{10}(x_i) = P_{01}(x_i) = \frac{E(x_i)}{2}$$

Eventually, the total dynamic power dissipation is given by:

$$P_{tot} = \frac{1}{2}V^2\left[C_{AND}\sum_{i=0}^{Q} E(x_i) + C_{OR}\sum_{j=1}^{M} E(y_j) + C_L E(F)\right] \qquad (4)$$

Where $x_i$is the $i^{th}$of the first level, $Q (Q \geq n)$ is the total number of the inputs of the first level, y_j is the $j^{th} output$ of the first level, M is the number of the AND gates, C_{AND} is the input capacitance of each primary input of an AND gate, C_{OR} is the input capacitance of each input of the OR gate, and C_L is the output load (Schoof, 2020).

2.2 Synthesis for Low Power

The basic principles of the proposed method, employing a certain logic function are presented first, while the formal description follows. It is assumed that signal x_3 of the logic function, $F = x_0x_1 + x_0x_2 + x_0x_3$ exhibits low transition probability and high static-1 probability, while the signals $x_0, x_1, and. x_2$ are characterized by high-transition probabilities. The corresponding logic circuit of the function F is shown in figure 8. When $x_3 = 1,$ the function can be expressed as:

$$F_{(x_3=1)} = x_0x_1 + x_0x_2 + x_0 = x_0$$

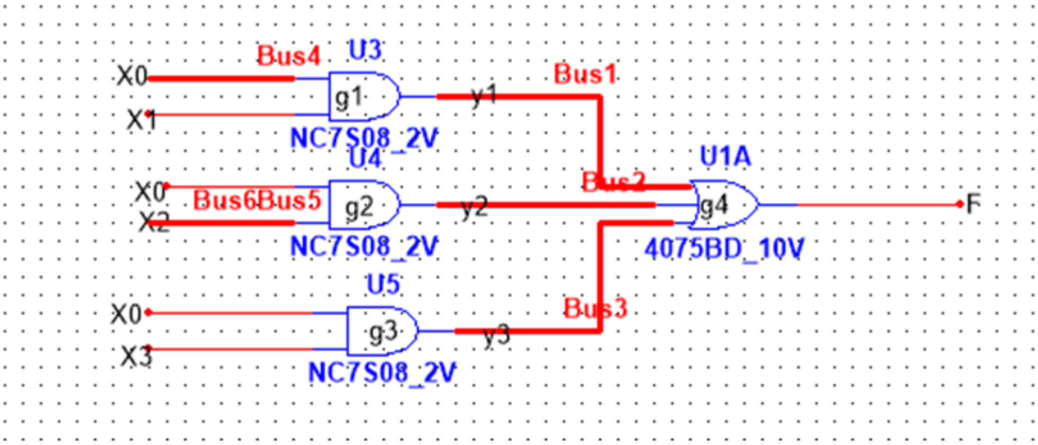


Figure 8. Logic circuit of function F. Source: Author, 2023.

During this time interval the value of the logic function depends only on the value of the interval nodey_3. More specifically, if $x_0 = 1$, the logic value of F is equal to 1 for any logic value of the nodes $y_1.and.y_2$. Hence, the corresponding power consumption of the nodes $y_1..and..y_2$ can be reduced, that is, energy can be conserved. Inserting the complement form of the signal x_3 into the first two terms of the logic function, a new logic expression,

$F' = x_0x_1\bar{x}_3 + x_0x_2\bar{x}_3 + x_0x_3$ Can be obtained as it is shown in Figure 9.

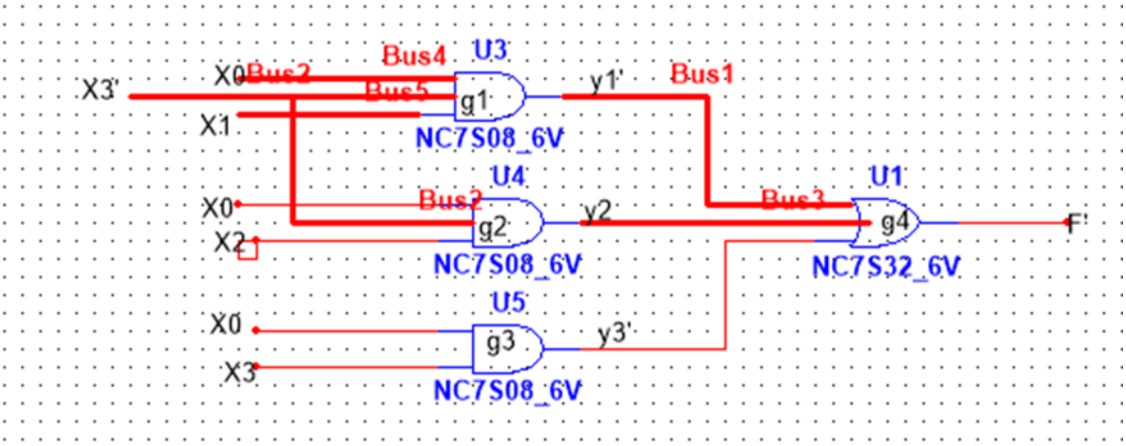
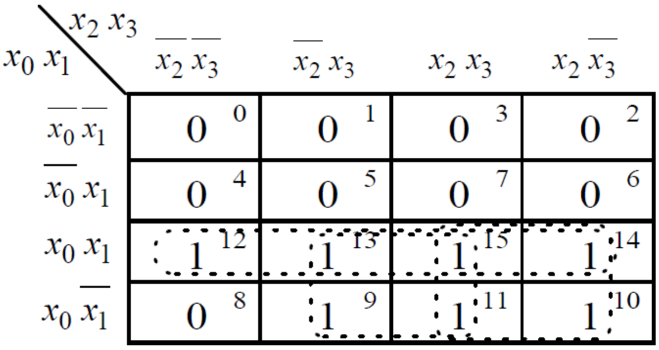


Figure 9. Shows a New Logic Expression. Source: Author, 2023.

In this circuit, if $x_3 = 1$, the logic values of nodes $y_1{}' and..y_2{}'$ are equal to zero and thus they do not make any transition. The functionality of the original circuit is preserved since $F'_{(x_3-1)} = F_{(x_3-1)} = x_0$ and $F_{(x_3-1)} = F_{(x_3-1)} = x_0x_1 + x_0x_2$

Consequently, selecting the signal x_3 as blocking variable, the logic operation remains unchanged, whereas the nodes $y_1{}' and..y_2{}'$dissipate fewer power compared with the starting form of the logic function. Applying the optimization tool to the set of minterms:

$F = \{9,10,11,12,13,14,15\} three.groups.of.min\,t\,erms \{12,13,15,14\},\{13,15,9,11\} and \{15,14,11,10\}$ Can be obtained as they are shown in Karnaugh map of Figure 10.



$x_0x_1 \backslash x_2x_3$	$\bar{x}_2\bar{x}_3$	$\bar{x}_2x_3$	x_2x_3	$x_2\bar{x}_3$
$\bar{x}_0\bar{x}_1$	0^{0}	0^{1}	0^{3}	0^{2}
$\bar{x}_0x_1$	0^{4}	0^{5}	0^{7}	0^{6}
x_0x_1	1^{12}	1^{13}	1^{15}	1^{14}
$x_0\bar{x}_1$	0^{8}	1^{9}	1^{11}	1^{10}

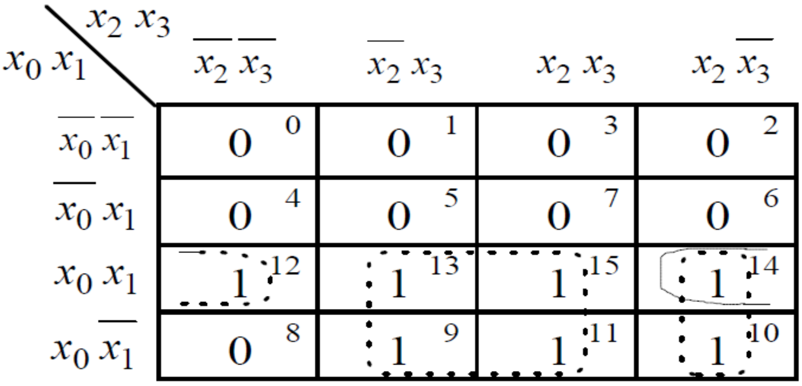
$F = x_0x_1 + x_0x_2 + x_0x_3$

Figure 10. Shows Karnaugh Map Illustration of Power logic optimization

Exploiting the statistical characteristics of the signal$\bar{x}_3$, this signal must appear as many times as possible in the terms of the function F. It can be proved that the subsets of the minterms:

$\{9,11,12,13,15\},\{12,14\} and \{10,14\}$result into the power optimized logic function:

$F' = x_0x_1\bar{x}_3 + x_0x_2\bar{x}_3 + x_0x_3$ as it is shown in Figure 11.



$x_0x_1 \backslash x_2x_3$	$\bar{x}_2\bar{x}_3$	$\bar{x}_2x_3$	x_2x_3	$x_2\bar{x}_3$
$\bar{x}_0\bar{x}_1$	0^{0}	0^{1}	0^{3}	0^{2}
$\bar{x}_0x_1$	0^{4}	0^{5}	0^{7}	0^{6}
x_0x_1	1^{12}	1^{13}	1^{15}	1^{14}
$x_0\bar{x}_1$	0^{8}	1^{9}	1^{11}	1^{10}

$F' = x_0x_1\overline{x_3} + x_0x_2\overline{x_3} + x_0x_3$

Figure 11. Power Optimization Logic Function. Source: Author, 2023.

Applying equation (4) for logic function $F..and..F'$ the corresponding total power dissipation are;

$$P_{tot_1} = \frac{1}{2}V^2 f(C_{AND}[3E(x_0) + E(x_2) + E(x_3)] + C_{OR}[E(y_1) + E(y_2) + E(y_3)] + C_L E(F)) \qquad (5)$$

$$P_{tot_2} = \frac{1}{2}V^2 f(C_{AND}[3E(x_0) + E(x_1) + E(x_2) + 3E(x_3)] + C_{OR}[E(y_1) + E(y_3)] + C_L E(F')) \qquad (6)$$

Respectively. Assuming $P(x_0 = 1) = 0.5, E(x_0) = 0.7. P(x_1 = 1) = 0.5, E(x_1) = 0.8$ $p(x_2) = 0.4, E(x_2) = 0.6, P(x_3) = 0.9, E(x_3) = 0.2$ and using equation (4), it can be obtained that $E(y_1) = 0.47, E(y_2) = 0.37, E(y_3) = 0.66, E(y_1) = 0.05, E(y_2') = 0.04, , and, , E(F) = E(F^{'}) = 0.5$ Then substituting the above values of the transition probabilities into equations (5) and (6) we obtain:

$$P_{tot_1} = \frac{1}{2}V^2 f(C_{AND}3.7 + C_{OR}1.5 + C_L 0.5) \qquad (7)$$

$$P_{tot_2} = \frac{1}{2}V^2 f(C_{AND}4.1 + C_{OR}0.75 + C_L 0.5) \qquad (8)$$ respectively.

Hence the expected total numbers of the transitions (over all nodes of each logic circuit per clock cycles:

$$E_1 = 3.7 + 1.5 + 0.5 = 5.7 \qquad (9)$$

$$E_2 = 4.1 + 0.75 + 0.5 = 5.35 \qquad (10)$$

respectively.

Apparently, the second logic implementation has reduced transition activity compared with the first one. Eventually, using equation (9) and (10), the resulting amount of the power saving is proportional to:

$$\frac{E_1 - E_2}{E_1} * 100\% = 6.14\% \qquad (11)$$

2.3. Clock Gating Execution

There is no need to clock a register when the "data" input is idle, so the "clock" can be gated to turn the register off. A signal known as the "clock gating enable" (Figure 12) can be used to gate the clock if it feeds a bank of registers (Hussein et al., 2018).

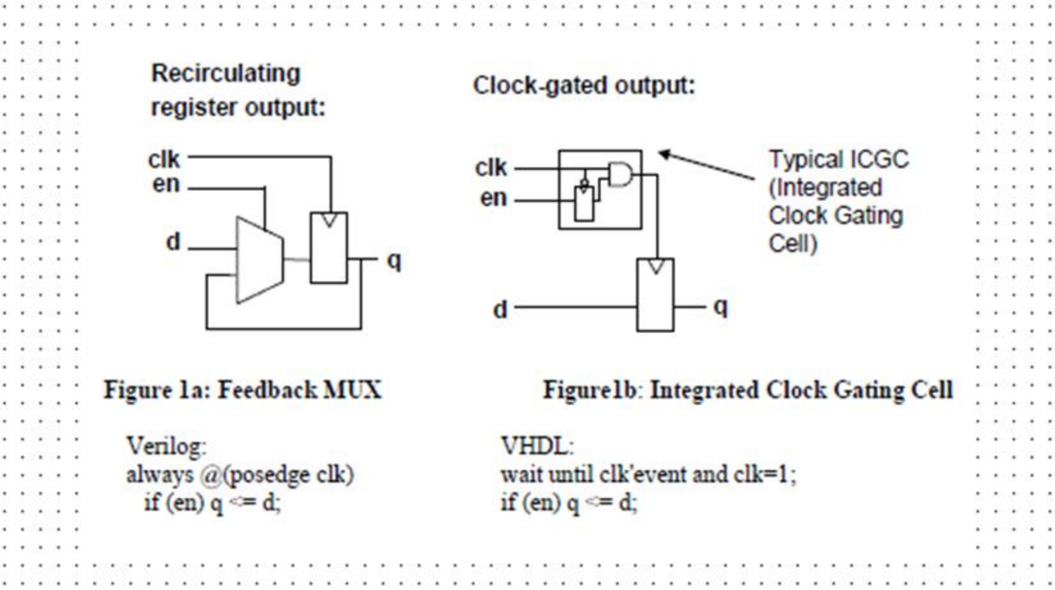

Recirculating register output:
clk
en
d
q
Clock-gated output:
clk
en
Typical ICGC (Integrated Clock Gating Cell)
d
q

Figure 1a: Feedback MUX

Figure1b: Integrated Clock Gating Cell

```
Verilog:
always @(posedge clk)
  if (en) q <= d;
```

```
VHDL:
wait until clk'event and clk=1;
if (en) q <= d;
```

Figure 12. RTL Code Examples with Enable. Source: Author, 2023.

As seen in Figure 12, synthesis tools may select between two alternative implementations when a "explicit" clock enable is present in the RTL code. In the "re-circulating register" method depicted in Figure 12a, the enable is used to either choose a new data value or re-circulate the existing data value. A "gated clock" implementation is what is depicted in Figure 12b. The clock is disabled when the enable is off. Although the output of the two solutions will never alter, their timing and power behavior will (Dhivakaran et al., 2022).

2.4. Clock Domain Crossings

For novel enabling and downstream gate-level clock gating methods, designers using automated RTL fixing should be aware of any potential issues with metastability on asynchronous clock domain crossings. Figure 13 shows a real-world design example where a clock gate was placed between two asynchronous clock domains by a power optimization tool, causing a design re-spin. Deploying an automated power-reduction solution that can determine whether new power-reduction opportunities are secure for clock domain crossover (CDC) is essential (Wei Jang, 2022).

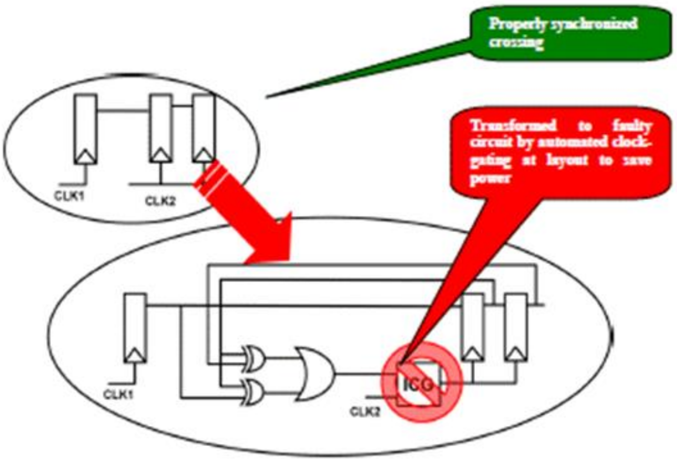

Properly synchronized crossing
Transformed to faulty circuit by automated clock-gating at layout to save power
CLK1
CLK2
CLK1
ICG
CLK2

Figure 13. Clock Gating Causing CDC Problems. Source: Author, 2023.

3. Evaluation

This switch has a threshold at which it will latch (stay on), making it light-sensitive. The latch can be reset using the S1 light-controlled switch circuit. The variable resistor R1 can be used to alter the threshold of light at which the circuit activates. The value of R1 is chosen to match the resistance of the photocells at night. Two circuits can be used to monitor an input, an output, or even the power supply rails. Any small spike, transient, or glitch will be recorded because the LED is always lit (Figure 14).

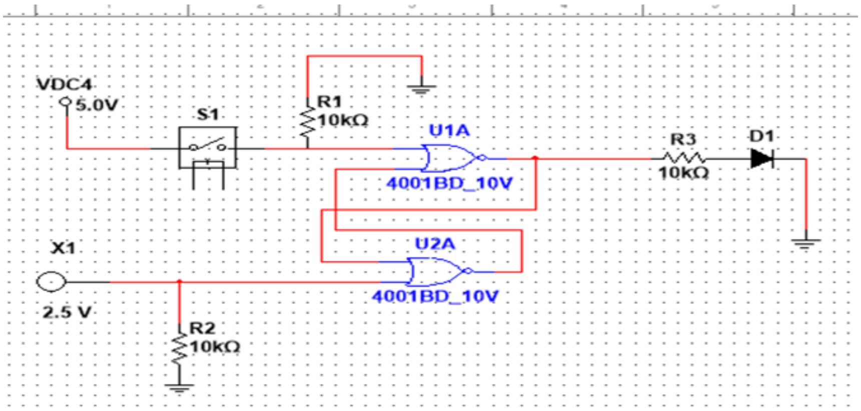


Figure 14. Positive Glitch Detector. Source: Author, 2023.

3.1. Flowchart Algorithm

The positive glitch detector needs two NOR gates. The gates are configured as SR (set reset) flip flops. Power sources include power supplies and the logic circuit that will be under observation. If an external power source is used, it must have an identical DC voltage to the system being tested and have its grounds connected in series. If the LED is lit after connection, pressing the reset switch will cause it to go out. The probe is then set up to look for any helpful mistakes. Any positive error will cause the output to latch high, the LED to turn on, and the SR flip-flop to be set (figure 15).

The input must switch from low to high within the CMOS IC's own transition time, which is typically 200 ns from a 5 Volt supply, according to the CD4001 data sheet. A long lead would increase capacitance and slow the response time, so it should be kept as short as possible. The probe can even be placed on a ground line or an output that is generally low. The LED turns on after any positive spike is detected and stays lit until it is reset.

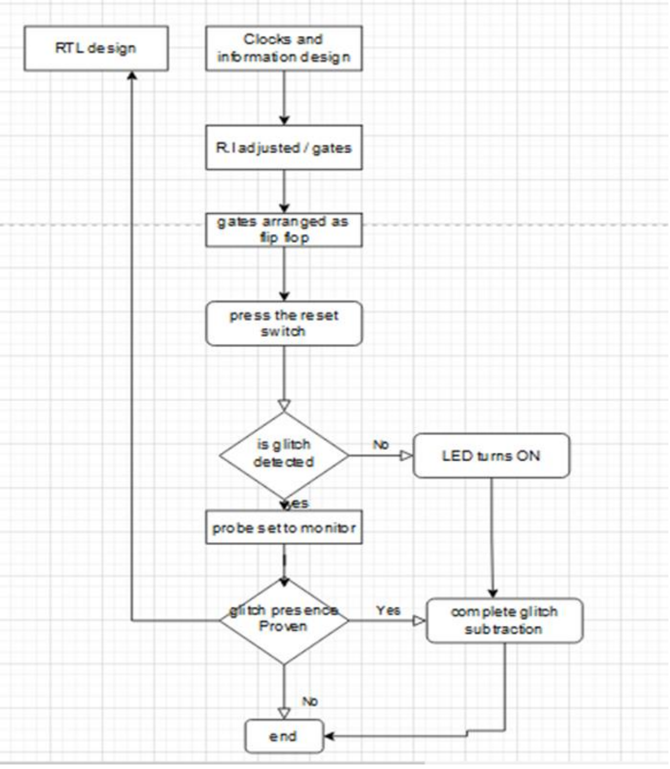


Figure 15. Flowchart for Glitch Monitor. Source: Author, 2023.

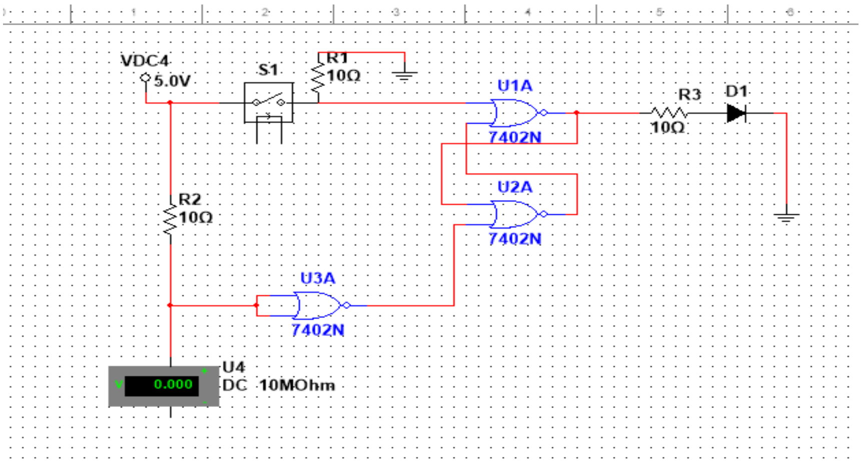


Figure 16. Negative Glitch Detector. Source: Author, 2023.

The negative glitch detector uses a second gate as an inverter and has a similar construction. The probe can be used to monitor the positive power supply bus or connected to an output or input pin that is generally kept in the positive position (fig 16). The SR flip flop will be activated by any negative transient or spike, turning on the output LED until it is reset. All open input pins should be connected to ground (Rovana et al., 2022).

4. Result and Discussion

The suggested algorithm analyzes the circuit from the principal inputs to the output nodes in a bottom-up manner. Two CMOS 4001 Quad NOR gates are used in the circuit. U2A forms a latch, and gate U1A serves as the trigger. S1 causes a circuit reset. When the switch is turned on, C1 sends a brief negative pulse to U1a's gate, assuming the light threshold has not been achieved. Unless the light threshold is achieved, at which point you should press S1, this will turn the latch off.

It causes a threshold voltage change that may result in a permissible increase in the total circuit delay, which is determined by subtracting the needed delay from the critical path delay of the circuit in its unaltered state. This approach effectively checks the differential path delay (DPD) of the input signals to each gate in the circuit to look for a potential glitch.

The maximum threshold voltage possible for High Threshold Voltage Low Power (HVTLP) transistors with a 1.2V substrate bias is employed for each glitchy gate. The program then advances to the following gate if the critical path delay still meets the delay requirements. Unless the delay limitations are conserved, the threshold voltage is controlled. The magnitude of the glitch will be decreased, even if it cannot be completely filtered, which will save energy.

5. Conclusion

The switching activity in the circuits is one of the main elements that affect how much power is consumed in CMOS combinational logic circuits. Such switching actions frequently result from false pulses, also known as glitches. In order to decrease overall power dissipation, this paper presents the technique of using clock gating with power gating in finite state machines (FSMs).

It describes an optimization method based on threshold voltage change for glitch power reduction. The goal is to reduce spurious transitions and, as a result, save energy by adjusting the threshold voltage of specific transistors of gates with eventual glitch occurrence. We create an algorithm that adjusts a circuit's netlist to remove glitches while maintaining the desired delay performance. A total energy savings of 6.14% and a leakage energy savings of 93.86% is achieved applying our method to C17 benchmark circuit.

6. Acknowledgement

I would like to express my heartfelt gratitude to my supervisor, Professor Akinwale A. T for his unwavering support and guidance throughout the research process. His expertise, insights, and encouragement were invaluable in helping to complete this work. I also want to thank my colleagues at Federal University of Agriculture Abeokuta Nigeria for their helpful feedback and support.

Finally, I would like to thank my son (Ehisoyayan Akhigbe-mudu Jnr) and my daughter (Mrs. Ebehitale Imariagbontua) alais, Iye Esosa for their love and support throughout the research process. Without their encouragement and support, I would not have been able to complete this research.

7. Authors' Contributions

Akhigbe-mudu Thursday Ehis: study design, conception, analyses, writing, corrections, submission and publication.

8. Conflicts of Interest

No conflicts of interest.

9. Ethics Approval

Not applicable.

10. References

Ahmadihosseini, Z., Moeinian, M., Nazemi, S., Elyasi, S., & Mohammadpour, A. H. (2020). Evaluation of the Correlation between the rs4918 Polymorphism of AHSG Gene and Coronary Artery Calcification in Patients with Coronary Artery Disease. *Cardiogenetics*, 10(2), 33-41. https://doi.org/10.3390/cardiogenetics10020007

Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2022). Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET. *IEEE Internet of Things Journal*, 10(10), 8477-849. https://doi.org/10.1109/JIOT.2022.3199712

Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2023). Falsification Detection System for IoV Using Randomized Search Optimization Ensemble Algorithm. *IEEE Transactions on Intelligent Transportation Systems*, 24(4), 4158-4172. https://doi.org/10.1109/TITS.2022.3233536

Boruga, R., & Megan, M. (2022). On Some Characterizations for Uniform Dichotomy of Evolution Operators in Banach Spaces. *Mathematics*, 10(19), 3704. https://doi.org/10.3390/math10193704

Cașcaval, P., & Leon, F. (2022). Optimization Methods for Redundancy Allocation in Hybrid Structure Large Binary Systems. *Mathematics*, 10(19), 3698. https://doi.org/10.3390/math10193698

Danquah, P., & Kwabena-Adade, H. (2020). Public Key Infrastructure: An Enhanced Validation Framework. *Journal of Information Security*, 11(4), 241-260. https://doi.org/10.4236/jis.2020.114016

Dhivakaran, P. B., Vinodkumar, A., Vijay, S., Lakshmanan, S., Alzabut, J., El-Nabulsi, R. A., & Anukool, W. (2022). Bipartite Synchronization of Fractional-Order Memristor-Based Coupled Delayed Neural Networks with Pinning Control. *Mathematics*, 10(19), 3699. https://doi.org/10.3390/math10193699

Guo, S., Yi, Z., Liu, P., Wang, G., Lai, H., Yu, K., & Xie, X. (2022). Analysis and Performance Evaluation of a Novel Adjustable Speed Drive with a Homopolar-Type Rotor. *Mathematics*, 10(19), 3712. https://doi.org/10.3390/math10193712

Gupta, T., & Akhter, S. (2021). *Design and Implementation of Area-Power Efficient Generic Modular Adder using Flagged Prefix Addition Approach*. In: 2021 7th International Conference on Signal Processing and Communication (ICSC) (pp. 302-307). IEEE. https://doi.org/10.1109/ICSC53193.2021.9673363

Jiang, W. (2022). Machine Learning Methods to Detect Voltage Glitch Attacks on IoT/IIoT Infrastructures. *Computational Intelligence and Neuroscience*, Article ID 6044071. https://doi.org/10.1155/2022/6044071

Khan, F., Zahid, M., Gürüler, H., Tarımer, İ., & Whangbo, T. (2022). An Efficient and Reliable Multicasting for Smart Cities. *Mathematics*, 10(19), 3686. https://doi.org/10.3390/math10193686

Kaptchuk, G., Massacci, F., Garcia, S. N. M., & Redmiles, E. M. (2022). Introduction to the Special Issue on Security and Privacy for COVID-19. *Digital Threats: Research and Practice (DTRAP)*, 3(3), 1-2. https://doi.org/10.1145/3549070

Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2019). Energy/area-efficient scalar multiplication with binary Edwards curves for the IoT. *Sensors*, 19(3), 720. https://doi.org/10.3390/s19030720

Maimuţ, D., & Matei, A. C. (2022). Speeding-Up Elliptic Curve Cryptography Algorithms. *Mathematics*, 10(19), 3676. https://doi.org/10.3390/math10193676

Mısır, O., & Akar, M. (2022). Efficiency and Core Loss Map Estimation with Machine Learning Based Multivariate Polynomial Regression Model. *Mathematics*, 10(19), 3691. https://doi.org/10.3390/math10193691

Mogheer, H. S., & Hasan, K. K. (2018). Implementation of Clock Gating for Power Optimizing in Synchronous Design. Tikrit Journal of Engineering Sciences, 25(3), 12-18. http://doi.org/10.25130/tjes.25.3.03

Pakkiraiah, C., & Satyanarayana, R. V. S. (2022). *Design of Low Power Modular (x mod p) Reduction Unit Based on Switching Activity for Data Security Applications*. In: Advances in VLSI and Embedded Systems: Select Proceedings of AVES 2021 (pp. 13-25). Singapore: Springer Nature Singapore.

https://doi.org/10.1007/978-981-19-6780-1_2

Schoof, R. (2020). On the ideal class group of the normal closure of Q (np). *Journal of Number Theory*, 216, 69-82. https://doi.org/10.1016/j.jnt.2020.04.004

Sghaier, A., Zeghid, M., Massoud, C., Ahmed, H. Y., Chehri, A., & Machhout, M. (2022). Fast Constant-Time Modular Inversion over F p Resistant to Simple Power Analysis Attacks for IoT Applications. *Sensors*, 22(7), 2535. https://doi.org/10.3390/s22072535

Shahbazi, K., & Ko, S. B. (2021). Area and power efficient post-quantum cryptosystem for IoT resource-constrained devices. *Microprocessors and Microsystems*, 84(7), 104280. https://doi.org/10.1016/j.micpro.2021.104280

Shanmugham, S. R., & Paramasivam, S. (2018). Survey on power analysis attacks and its impact on intelligent sensor networks. *IET Wireless Sensor Systems*, 8(6), 295-304. https://doi.org/10.1049/iet-wss.2018.5157

Shah, N. A., Alyousef, H. A., El-Tantawy, S. A., Shah, R., & Chung, J. D. (2022). Analytical investigation of fractional-order Korteweg–De-Vries-type equations under Atangana–Baleanu–Caputo operator: Modeling nonlinear waves in a plasma and fluid. *Symmetry*, 14(4), 739. https://doi.org/10.3390/sym14040739

Sun, G., Chen, C. C., & Bin, S. (2021). Study of cascading failure in multisubnet composite complex networks. Symmetry, 13(3), 523. https://doi.org/10.3390/sym13030523

Sun, D. Z., & Tian, Y. (2022). Member Tampering Attack on Burmester-Desmedt Group Key Exchange Protocol and Its Countermeasure. *Mathematics*, 10(19), 3685. https://doi.org/10.3390/math10193685

Theodoridis, G., Theoharis, S., Soudris, D., & Goutis, C. E. (1998). Method for minimising the switching activity of two-level logic circuits. *IEE Proceedings-Computers and Digital Techniques*, 145(5), 357-363. https://doi.org/10.1049/ip-cdt:19982203

Varghese, J., & Sreekala, K. S. (2019). Clock-Gating: A Novel Method for Reducing Dynamic Power Dissipation on FPGAS. *International Journal of Engineering Research & Technology (IJERT)*, 8(5), 917-922. https://doi.org/10.17577/IJERTV8IS050527

Xu, W., Zhu, Q., & Zhao, L. (2022). GlitchNet: A glitch detection and removal system for SEIS records based on deep learning. *Seismological Society of America*, 93(5), 2804-2817. https://doi.org/10.1785/0220210361

Copyrights