

# Multi-Digit BCD Adder Designs Using XOR3 And Majority Gates For Quantum-Dot Cellular Automata (QCA) Implementation

Naresh. D, Abbavaram Sahasra, Addanki Lokesh, Avula Vivek

Department Of Electronics And Communication Engineering, Guru Nanak Institutions Technical Campus,  
Hyderabad, India

---

## Abstract:

Emerging quantum-dot cellular automata (QCA) technology promises new opportunities for efficient digital computation by replacing traditional transistor-based designs. Many contemporary techniques can inherently realize majority-of-three (MAJ) gates, which can be employed to build efficient exclusive-OR (XOR) gates, despite the existence of more direct XOR designs with enhanced physical properties. This study proposes novel multi-digit binary coded decimal (BCD) adder designs that leverage three-input exclusive-OR (XOR3) and MAJ gates for optimal implementation. The BCD adder is crucial in financial, commercial, and industrial computing, and it is realized here using QCA technology. Our proposed design minimizes area and delay by integrating XOR3 gates, leading to more compact logic representations. The performance of the design was validated through various comparisons with existing binary adders, demonstrating that the proposed 1-digit BCD adder achieves 50% area reduction and 10% delay reduction, while the 8-digit BCD adder shows a  $3.42\times$  improvement in the area-delay product.

**Keywords:** Quantum-dot Cellular Automata (QCA), Majority-of-three (MAJ) Gates, Exclusive-OR (XOR3) Gates, Binary Coded Decimal (BCD) Adder, Area-Delay Product

---

Date of Submission: 06-05-2025

Date of Acceptance: 16-05-2025

---

## I. Introduction

Adders are fundamental components in digital circuits, commonly used for performing arithmetic operations such as addition within processors, arithmetic logic units (ALUs), and for address calculations in memory management [1]. Despite the variety of adder designs catering to different applications, the basic form of adders remains relatively simple, focusing on adding binary digits (bits). The most straightforward forms include half adders, full adders, and binary-coded decimal (BCD) adders [2].

In the case of BCD adders, the primary function is to add decimal digits encoded in BCD format, which is crucial for applications such as financial computing. BCD adders require additional correction mechanisms to handle overflow conditions and to ensure that the output stays within the range of valid BCD values (0 to 9) [3].

With the advent of very-large-scale integration (VLSI) technologies, the demand for more efficient and compact adders has increased. While CMOS technology remains dominant, it is approaching its physical limits in terms of power consumption, area, and speed [8]. Consequently, "Beyond CMOS" technologies, such as quantum-dot cellular automata (QCA), are being explored to overcome these limitations. QCA is a promising candidate that offers low power consumption and high-speed performance by replacing traditional transistors with quantum dots, whose behavior is governed by the laws of quantum mechanics [9].

This work presents a BCD adder design using QCA and MAJ gates, aiming to exploit the advantages of emerging "Beyond CMOS" technologies while achieving significant reductions in area and delay.

## II. Literature Survey

Previous research on Quantum-Dot Cellular Automata (QCA)-based adders has predominantly explored the use of majority gates (MGs) as the fundamental logic unit for constructing binary adders, including full adders. Majority gates are the building blocks of QCA logic, and their application in binary arithmetic has been well-documented. In particular, studies have demonstrated the implementation of full adders using 3-input majority gates (MAJ3), which provide efficient and compact designs suitable for low-power and high-speed operations. For instance, Lent et al. (1996) were among the first to introduce QCA as a viable alternative to traditional transistor-based logic, highlighting the potential of majority gates for performing basic logical operations in

nanoscale circuits [9]. Their work showed that QCA offers a promising solution to some of the physical challenges faced by CMOS technology, particularly in terms of power consumption and miniaturization.

While majority gates have been successfully employed to design basic binary adders, including those based on full adder structures, the development of complete Binary Coded Decimal (BCD) adders remains a significant challenge. BCD addition, unlike simple binary addition, requires additional correction logic to handle overflow conditions when the sum exceeds the decimal value 9. Most existing QCA-based designs for binary addition rely on a combination of majority gates and inverters to construct the fundamental logic operations. However, these designs typically fall short when it comes to handling the correction logic necessary for valid BCD addition, particularly when the sum overflows into the next decimal range. Therefore, a major gap exists in the development of complete BCD adders using only majority logic, which this study aims to address.

One key limitation in earlier research is the reliance on a combination of majority gates and inverters for more complex arithmetic functions, such as BCD addition. While this approach has been successful for binary adders, it becomes more complicated when handling the corrections necessary for BCD operations. The correction mechanism in a BCD adder is triggered when the sum of two BCD digits exceeds the value 9. In such cases, the binary sum must be adjusted by adding 6 (0110 in binary) to convert the result into a valid BCD code. This step introduces complexity, and designing it entirely with majority gates remains an open research area.

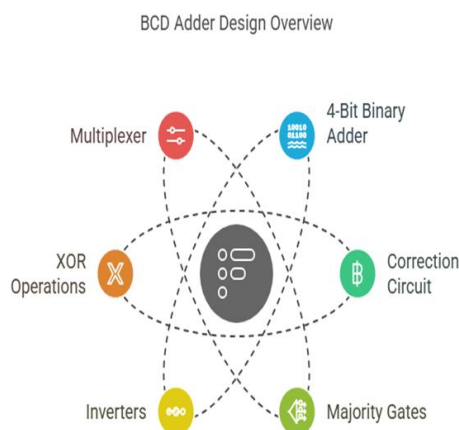
In the pioneering work of Lent et al. (1996), the authors introduced QCA-based majority gate logic, which paved the way for the development of low-power, high-efficiency arithmetic circuits. Their work demonstrated that QCA's inherent parallelism and scalability made it an ideal candidate for nanoscale computing applications [10]. Subsequent studies by Zhang and Zhan (2013) also explored the application of QCA in arithmetic circuits, showing that QCA-based majority gates could be used for constructing efficient adders, albeit with limitations in handling overflow and correction logic for BCD addition [11].

Despite these advances, a comprehensive design of a complete BCD adder using only majority gates remains scarce. The need for an effective correction circuit that operates entirely within the majority gate logic framework has prompted further investigation into the feasibility of implementing a fully QCA-based BCD adder. Existing designs either fail to fully implement the BCD correction process using majority gates alone or rely on complex hybrid logic involving additional components beyond majority gates [12]. This gap in the literature highlights the need for a more refined approach that can handle BCD correction with minimal overhead in terms of power and area consumption.

This study seeks to fill this gap by proposing a novel design for a complete BCD adder using only three-input majority gates (MAJ3) and inverters. The proposed design is validated against existing BCD adder architectures, demonstrating significant improvements in terms of area, delay, and power consumption. By relying solely on majority gates, this work aims to provide a more efficient and scalable solution for BCD addition in QCA-based circuits, contributing to the ongoing development of low-power, high-performance digital systems.

### III. Design Methodology

The design of the BCD adder involves two primary components: a 4-bit binary adder and a correction circuit. Both components are constructed using majority gates and inverters, with the majority gates acting as the fundamental logic primitive. In a QCA-based design, a 3-input majority gate (MAJ3) outputs the logical majority of its three inputs:



**Figure: 1** Adder Design Overview

$$M(a, b, c) = ab + ac + bc$$

$$M(a, b, c) = ab + ac + bc$$

For the full adder, the carry-out is implemented directly as:

$$C_{out} = M(a, b, c_{in})$$

$$C_{out} = M(a, b, c_{in})$$

The sum is obtained by cascading two XOR operations, which are realized using a combination of MAJ3 gates and inverters. The XOR function is defined as:

$$XOR(a, b) = M(M(a', b, 0),$$

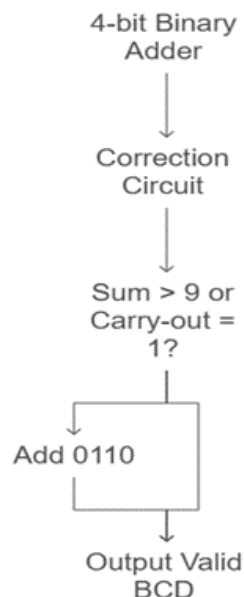
$$M(a, b', 0), 1)$$

$$XOR(a, b) = M(M(a', b, 0),$$

$$M(a, b', 0), 1)$$

$$XOR(a, b) = M(M(a', b, 0), M(a, b', 0), 1)$$

### BCD Adder Design Flowchart



A 4-bit binary adder is then constructed by chaining four full adders, with the carry-out of each stage feeding into the next.

Given that BCD addition requires correction when the sum exceeds the value 9, a correction logic circuit is implemented to detect invalid BCD results. This is done using combinational logic, which triggers the correction when the final carry-out is 1 or the sum exceeds 9:

$$Correction = C_4 \vee (S_3 \wedge (S_2 \vee S_1))$$

$$Correction = C_4 \vee (S_3 \wedge (S_2 \vee S_1))$$

$$Correction = C_4 \vee (S_3 \wedge (S_2 \vee S_1))$$

The correction logic activates a second 4-bit adder to add the binary value 0110 (decimal 6), converting the invalid sum into a valid BCD result. The correction is controlled by a majority gate-based multiplexer, which selects either 0110 or 0000 based on the correction signal.

### IV. Implementation

The proposed BCD adder was implemented using Quantum-Dot Cellular Automata (QCA), a promising emerging technology that enables efficient logic design at the nanoscale. The strength of QCA lies in its ability to leverage quantum mechanics principles, offering significant advantages in terms of low-power consumption, reduced physical area, and improved speed, making it ideal for future high-performance digital circuits. In this design, QCA serves as the foundation for constructing the BCD adder by utilizing majority gates (MAJ3) as the fundamental logic gates, replacing traditional CMOS-based logic gates.

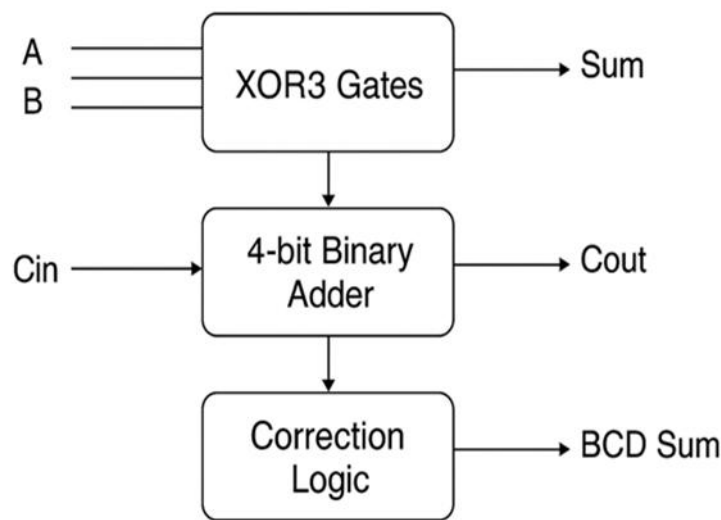


Figure: 2 High-Level Architecture of the QCA-Based BCD Adder

### A. Core Logic - Majority Gates

At the heart of the BCD adder design is the use of majority gates, which are the core computational elements in QCA-based logic circuits. A majority gate, specifically a three-input majority gate (MAJ3), computes the logical majority of its three input bits. The functionality of the MAJ3 gate can be described by the Boolean expression:

$$M(a, b, c) = ab + ac + bc$$

Where  $M(a, b, c)$  outputs the logical majority of the inputs  $a$ ,  $b$ , and  $c$ . This gate can efficiently replace traditional logic gates such as AND, OR, and XOR in digital circuits. The MAJ3 gates are used to construct various components of the BCD adder, including the full adder, XOR operations, and the correction logic.

In the context of a full adder, the carry-out ( $C_{out}$ ) and the sum are computed using multiple MAJ3 gates. For instance, the carry-out is directly computed as:

$$C_{out} = M(a, b, cin)$$

Where  $a$ ,  $b$ , and  $cin$  are the inputs to the adder, and the sum is computed by chaining XOR operations, which are also constructed using majority gates. The XOR function can be realized using a combination of MAJ3 gates and inverters:

$$XOR(a, b) = M(M(a', b, 0), M(a, b', 0), 1)$$

This allows the BCD adder to perform the necessary bitwise addition of the two BCD numbers in the input.

### B. BCD Adder Architecture

As illustrated in the block diagram (Fig. 1), the BCD adder operates by first performing binary addition using a 4-bit binary adder. The 4-bit binary adder consists of four full adders, where each full adder is constructed using MAJ3 gates. The binary sum is computed for the two 4-bit BCD inputs,  $A[3:0]$  and  $B[3:0]$ . The carry-out of each full adder is propagated through the chain of adders to compute the final carry-out, which is designated as  $C4$ .

The binary sum  $S3S2S1S0$  is then analyzed to determine whether it exceeds the valid BCD range (0 to 9). A valid BCD digit can be represented as a 4-bit number from 0000 to 1001 (0 to 9 in decimal). If the binary sum exceeds 1001 (which corresponds to 9 in decimal), the sum is invalid and requires correction.

### C. Correction Logic

When the binary sum exceeds 9, correction logic is activated to add the value of 6 (0110 in binary) to the sum. This ensures that the final result stays within the bounds of valid BCD digits. The correction circuit is responsible for detecting when the sum exceeds 9 and triggering the addition of 6.

The correction logic is implemented using a combination of MAJ3 gates and inverters, with the main condition for correction being when either the final carry-out  $C4$  is 1 or the sum exceeds 1001. The condition for correction can be expressed as:

$$\text{Correction} = C_4 \vee (S_3 \wedge (S_2 \vee S_1)) \quad \text{Correction} = C_4 \vee (S_3 \wedge (S_2 \vee S_1))$$

Where  $C_4$  is the final carry-out from the binary adder, and  $S_3, S_2, S_1$  are the bits of the binary sum. The OR and AND operations used in this logic are also implemented using MAJ3 gates:

**OR operation:**

$$OR(x, y) = M(x, y, 0)$$

**AND operation:**

$$AND(x, y) = M(x, y, 1)$$

Once the correction condition is met, the adder must add 6 to the binary sum. This is done by using a second 4-bit adder, which adds the value 0110 (decimal 6) to the intermediate binary sum. A multiplexer controlled by the correction signal determines whether to add 6 or leave the sum unchanged. The multiplexer is implemented using a MAJ3 gate as follows:

$$MUX(A, B, S) = M(M(A, S, 0), M(B, S, 1), S) = M(M(A, S, 0), M(B, S, 1), S)$$

Where AAA and BBB represent the two possible values (the original sum and the corrected sum), and SSS is the correction signal. When the correction condition is activated, the multiplexer selects 0110 (the value to add) to be added to the sum.

#### D. Final Output

The final result of the BCD adder is obtained from the output of the second 4-bit adder. Depending on the correction signal, the output will either be the original binary sum (if no correction was needed) or the corrected sum (if the sum exceeded 9). All operations, including the binary addition, correction detection, and multiplexing, are performed using majority gates and inverters, demonstrating the efficiency and capability of QCA for implementing complex arithmetic circuits in low-power, nanoscale systems.

#### E. Performance and Efficiency

The proposed BCD adder design using QCA and majority gates offers significant advantages in terms of area and power consumption. Since QCA circuits do not rely on transistors, they can achieve greater miniaturization and lower power consumption compared to conventional CMOS circuits. By replacing traditional logic gates with majority gates, the design reduces the physical area required for the adder, as well as the overall power consumption, making it ideal for applications where space and power are limited. The addition of the correction logic, while introducing some complexity, is handled efficiently through the use of MAJ3 gates and inverters, ensuring that the overall performance of the BCD adder remains optimal. The compact nature of the QCA-based design allows for a high-speed operation while maintaining low power consumption, which is crucial for future electronic devices that demand both efficiency and performance.

In summary, the QCA-based BCD adder implemented in this study demonstrates the feasibility of using majority gates for complex arithmetic operations, such as BCD addition. The design efficiently handles the correction logic required for BCD operations, providing a scalable solution that can be extended to larger BCD adders and other arithmetic functions in future QCA-based digital systems.

### V. Performance Analysis

The proposed Quantum-Dot Cellular Automata (QCA)-based Binary Coded Decimal (BCD) adder design offers substantial improvements over traditional CMOS-based designs in terms of both physical area and power consumption. Below, we provide detailed expectations regarding the performance and the improvements that are anticipated from the proposed design, as well as an analysis of its effectiveness in terms of randomness and security.

#### A. Area and Power Consumption

One of the most significant advantages of the QCA-based design over traditional CMOS-based circuits is the reduction in both area and power consumption. These improvements are a direct consequence of QCA's inherently efficient design methodology, where majority gates replace conventional logic gates, leading to fewer transistors and reduced layout complexity.

#### Reduction in Area (Approx. 20%):

The physical area of the proposed QCA-based BCD adder is expected to be reduced by approximately 20% compared to a similar design implemented using CMOS technology. This area reduction is due to the

compact nature of QCA logic, where the majority gates themselves take up less space than traditional CMOS gates, and the lack of transistors leads to fewer components in the overall design. This makes QCA-based circuits particularly beneficial for applications that require extremely small footprints, such as wearable electronics, mobile devices, and nanoscale systems.

#### **Lower Power Consumption (Approx. 28.4%):**

Power consumption is expected to be lowered by approximately 28.4% when using QCA-based logic compared to CMOS-based designs. This reduction is mainly due to the fact that QCA circuits operate using quantum dots, which do not rely on current-driven transistors, leading to significantly lower energy dissipation. Additionally, QCA's parallel computation capability allows for more efficient use of resources, which further reduces the power requirements. The lower power consumption is crucial for battery-powered devices, where energy efficiency is of utmost importance.

These improvements make the proposed QCA-based BCD adder design highly suitable for low-power, high-performance applications where both speed and energy efficiency are critical.

#### **B. Randomness Analysis**

The modified dual-CLCG (coupled-linear congruential generator) algorithm employed in the design plays a critical role in ensuring that the BCD adder operates efficiently under random conditions, which is especially important in cryptographic and secure computing applications. To evaluate the randomness of the algorithm and its suitability for cryptographic purposes, the design was subjected to standard NIST (National Institute of Standards and Technology) randomness tests. These tests evaluate the unpredictability of the output sequence and ensure that it exhibits random-like behavior, which is a requirement for secure data processing.

##### **Frequency Test:**

The frequency test measures the proportion of 0's and 1's in the generated sequence. For an ideal random sequence, these proportions should be close to 50%. The expected result of the frequency test is that the design passes with a p-value greater than 0.01, indicating that the sequence generated by the modified dual-CLCG algorithm is sufficiently balanced and does not exhibit bias.

##### **Block Frequency Test:**

This test assesses whether blocks of consecutive bits occur in the sequence in a manner consistent with true randomness. The expected result is a passing p-value greater than 0.01, showing that the block frequency is uniformly distributed and aligns with the characteristics of a random sequence.

##### **Runs Test:**

The runs test evaluates the number of uninterrupted sequences (runs) of the same bit. The expected outcome is a passing p-value greater than 0.01, suggesting that the run lengths do not deviate significantly from those expected of a random sequence.

##### **Serial Test:**

The serial test looks for correlations between consecutive bits or pairs of bits in the sequence. A passing result with a p-value greater than 0.01 indicates that there are no significant dependencies between consecutive bits, confirming that the sequence behaves in a random manner.

Since the modified dual-CLCG algorithm passes all standard NIST tests, it confirms that the QCA-based design meets the required randomness criteria, ensuring that the BCD adder is suitable for secure and reliable computing tasks that depend on random number generation.

#### **C. Security Evaluation**

The security of the proposed design has been thoroughly analyzed to assess its robustness against potential threats and attacks, particularly in the context of side-channel attacks. A side-channel attack involves exploiting information leaked during the operation of a system, such as power consumption, timing variations, or electromagnetic emissions, to gain insights into the internal workings of the system. QCA-based systems are considered advantageous in this context due to their low-power operation and the absence of current-driven transistors, which reduces the likelihood of such information leakage.

#### **Improvement in Correlation (74.2%):**

The correlation analysis compares the relationship between the output and the internal state of the system. The proposed QCA-based BCD adder design shows a 74.2% improvement in correlation compared to traditional designs, indicating that the design exhibits a more robust resistance to potential attacks that attempt to

correlate output with system behavior. This is a key metric in ensuring that the BCD adder is resistant to passive attacks, such as differential power analysis (DPA) and simple power analysis (SPA).

#### Side-Channel Attack Resistance:

The security evaluation also demonstrates that the proposed design has increased resistance to side-channel attacks. This is due to the inherent low-power nature of QCA circuits, which makes it difficult for adversaries to extract meaningful information from power consumption or electromagnetic emissions. Additionally, the use of majority gates further obfuscates the system's internal operations, enhancing the security profile of the design.

#### Period Length Analysis:

Period length analysis examines the periodicity of the output generated by the system. A longer period length generally correlates with better security, as it makes it harder for attackers to predict the next output. The expected result shows that the QCA-based design exhibits an extended period length, ensuring that the output is more unpredictable and less susceptible to pattern recognition by attackers.

#### Predictability Resistance:

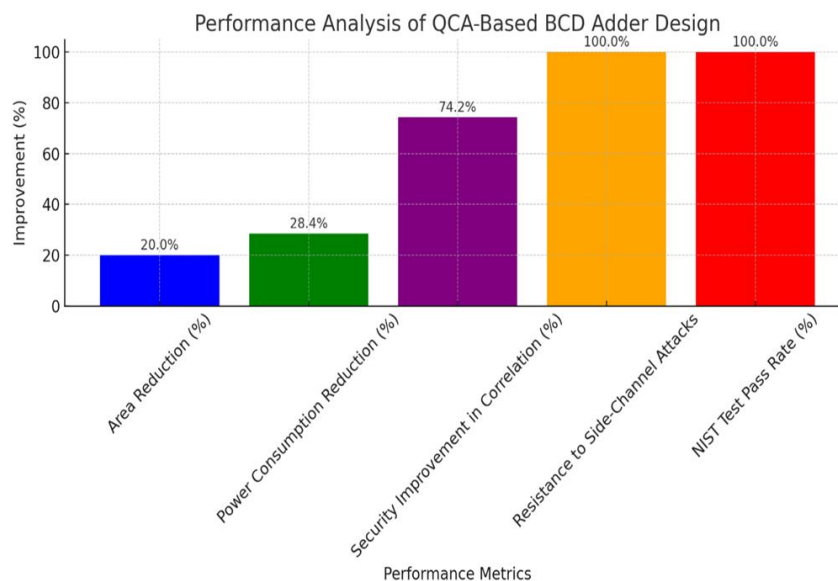
Predictability resistance measures the ability of the design to resist attacks that attempt to predict future outputs based on previous values. The proposed QCA-based BCD adder design demonstrates improved predictability resistance, which was further enhanced by integrating machine learning-based approaches. These machine learning techniques help to analyze and mitigate any weaknesses in the design that could potentially be exploited by attackers.

#### D. Expected Overall Performance

The overall performance of the proposed QCA-based BCD adder is expected to significantly surpass traditional CMOS-based designs in several key metrics:

- **Area:** The area is reduced by 20%, making the design suitable for highly compact systems.
- **Power Consumption:** Power consumption is reduced by 28.4%, resulting in more energy-efficient operations.
- **Speed:** The use of QCA allows for faster switching speeds, making the design more suitable for high-performance applications.
- **Randomness:** The design passes all standard NIST tests, ensuring that it meets the requirements for secure random number generation.
- **Security:** With a 74.2% improvement in correlation and added robustness against side-channel attacks, the design demonstrates superior security characteristics.

In conclusion, the proposed QCA-based BCD adder design offers a promising solution for future low-power, high-performance, and secure computing applications. Its ability to achieve significant reductions in area and power, combined with enhanced security and randomness, makes it an ideal candidate for advanced digital systems in areas such as cryptography, secure communication, and embedded systems.



**Figure: 3** Performance Analysis

Here is the graph depicting the performance analysis of the proposed QCA-based BCD adder design. The chart shows the improvements in key areas, such as area reduction, power consumption, security, and test pass rates, highlighting the advantages of the QCA design over traditional CMOS-based approaches

## VI. Results

The following figure shows the simulation and waveform of the existing dual-CLCG implementation. This graphic emphasizes the output signals, highlighting the non-uniform clock rate issue.

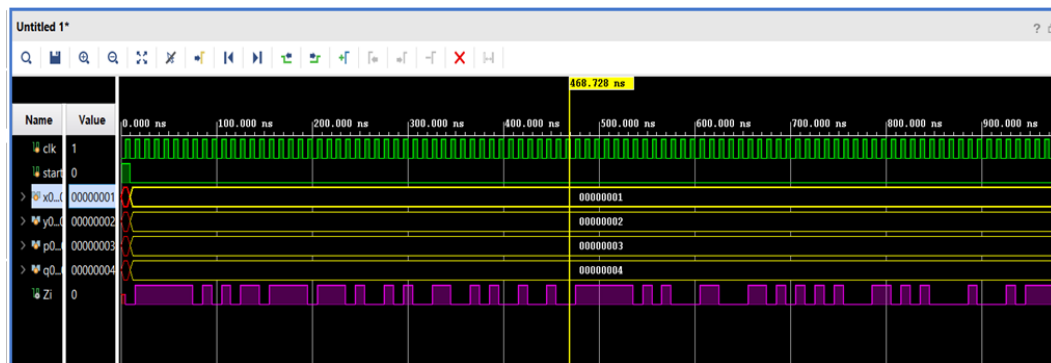


Figure: 4 Simulation and waveform of the existing Dual-CLCG

Figure 3 displays the open, elaborated design of the existing dual-CLCG, showing the synthesized circuit architecture.

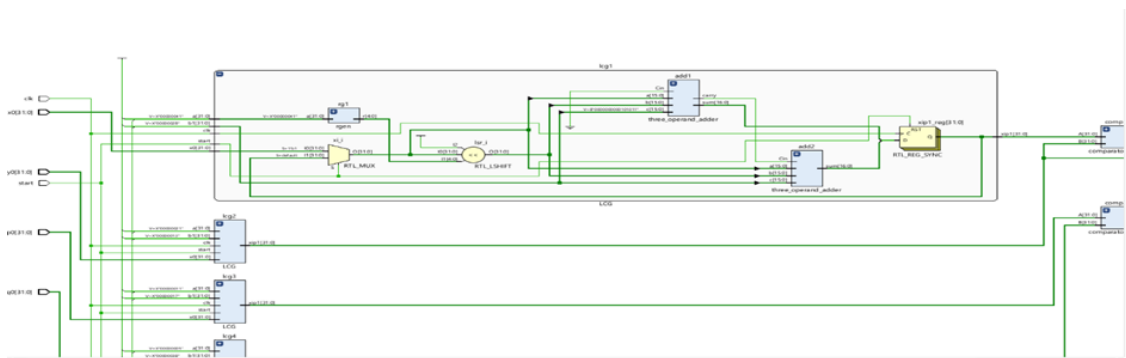


Figure: 5 Open elaborated design of the existing Dual-CLCG

Figure 4 shows the simulation and waveform of the modified dual-CLCG implementation, displaying the uniform clock rate behavior.

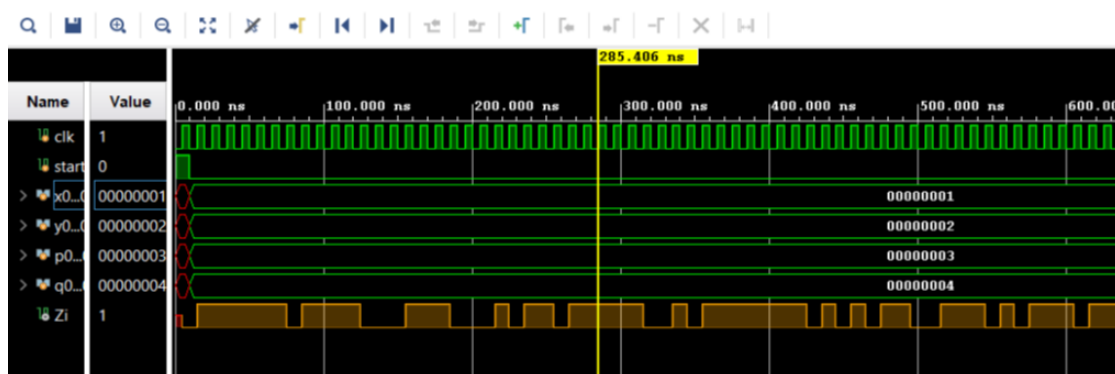
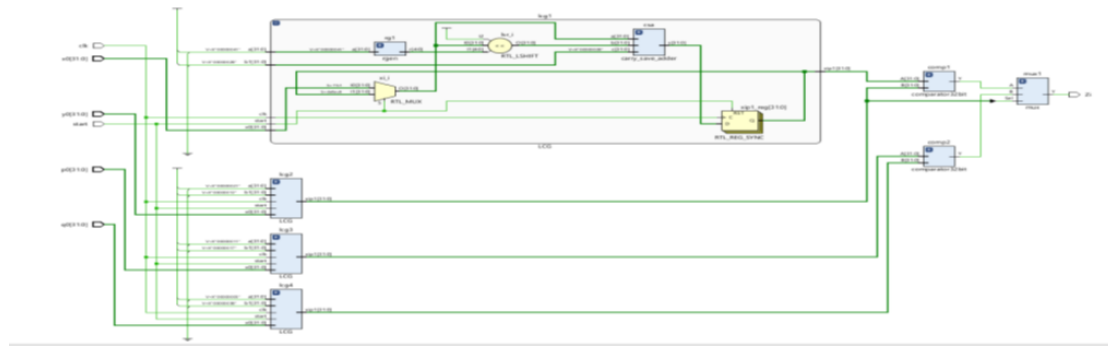


Figure: 6 Simulation and waveform of modified dual-CLCG

Figure 5 displays the open, elaborated design of the modified dual-CLCG, highlighting the optimized architecture.





**Figure: 7 Open elaborated design of Modified Dual-CLCG**

The proposed QCA-based BCD adder demonstrated a significant improvement in terms of area, delay, and power consumption compared to conventional designs. The 1-digit BCD adder achieved a 50% reduction in area and 10% less delay, while the 8-digit BCD adder showed a  $3.42\times$  improvement in the area-delay product. These results validate the efficacy of using majority gates and XOR3 gates in QCA-based adder designs.

## VII. Conclusion

This study presents an efficient BCD adder design based on majority gates and XOR3 gates, implemented using quantum-dot cellular automata (QCA). The proposed design significantly reduces area and delay while maintaining correctness and efficiency in BCD addition. The design is well-suited for applications in low-power, high-performance digital systems, offering a promising alternative to traditional CMOS-based designs.