

FPGA-Based Design and Implementation of a Reliable Electronic Voting System

¹Padmaja C, ²Dr. T. Kishore Kumar

¹Assistant Professor, ²Professor

¹Dept. Of ECE, GNITS, Hyderabad, India

¹c.padmaja@gnits.ac.in

Abstract: Polling using Electronic Voting Machines (EVMs) provides a more efficient, safe, and secure method, significantly reducing the time required compared to traditional methods. The proposed digital EVM, designed using Xilinx ISE with Verilog HDL, further enhances these benefits and can be implemented on an FPGA board for real-time application. This advanced EVM design involves multiple stages: initially, determining the total number of voters and contestants; then, enabling voting through an active high input signal for each voter, allowing them to cast their vote securely via a voter switch input. The design process includes creating a flowchart, developing algorithms, and writing code to implement and simulate the logic, ensuring a streamlined and reliable election process. In stage two, voting process begins when the voter casts his vote to a particular party or contestants the polled vote is registered in the individual contestant registry. In stage three after completion of voting process the votes are validated by comparing the votes polled to the contestants in their registries after which the election process ends by declaring the winner. The above proposed method can be implemented on FPGA board for real time applications ranging from university level elections to Assembly and Lok Sabha elections, as it has the advantage that it can be reprogrammed over and over for various tasks according to their requirement which helps in reducing the expenditure.

IndexTerms - EVM, Verilog HDL, FPGA, Xilinx, Validation, Security, Election, Reprogrammable.

I. INTRODUCTION

In a democratic system, voting serves as the fundamental process through which citizens elect their representatives. Hence, it must be executed with the highest level of accuracy and integrity to ensure that the selection reflects the true will of the people. Traditionally, elections were carried out using paper ballots, where voters indicated their choice by marking their preferred candidate's name. However, this manual approach posed several challenges, including vote tampering, counting errors, and biased outcomes.

To overcome these limitations, the Electronic Voting Machine (EVM) was introduced as a technological alternative. Despite its advantages, early EVM models that utilized removable memory cards were vulnerable to security breaches, as unauthorized access could enable manipulation of stored data. To enhance both the security and reliability of the voting process, a more robust electronic voting mechanism is essential. In this context, an Electronic Voting Machine has been designed using Verilog HDL and implemented on an FPGA platform through Xilinx ISE, offering improved protection against data tampering and ensuring trustworthy election results.

K. Gurucharan, ET.AL, [1] discussed in their paper the concept of an electronic mechanical voting device designed to automate the voting process without the need for manual ballot papers. They emphasized that the right to vote is fundamental in any democracy. In traditional elections, voters marked their choices using physical ballots, a time-consuming and error-prone process that could potentially compromise the fairness of the election. Their study underlined the inefficiencies of the manual voting system and laid the groundwork for developing electronic alternatives.

May, P., Ehrlich, H.C., Steinke, T [2] illustrated the implementation of electronic mechanical devices within the digital domain as a solution to the limitations of traditional voting systems. They argued that digital systems are more secure and less vulnerable to tampering, thus making the electoral process more reliable, efficient, and fair. Their approach aimed to modernize elections using electronic systems to uphold the integrity of democratic processes.

Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C. [3] highlighted the inefficiencies and high error potential in conventional election procedures. Their paper introduced a programmable electronic mechanical device designed to accept multiple votes from a single voter, addressing the specific needs of elections like those in Grama Panchayath and Cooperative Societies, where voters are required to select multiple candidates. They also incorporated a mode control feature, enabling the device to be configured for single or multiple vote casting as per the election type. The key advantage of this system is the prevention of invalid votes, especially in elections requiring multiple candidate selection.

Foster, I., Kesselman, C., Nick, J., Tuecke, S [4] described the implementation of secured electronic voting machines integrated with biometric authentication. These advanced systems utilize cutting-edge technologies to ensure that votes are cast only by legitimate voters, thereby enhancing the security and integrity of the election process. Biometric systems help prevent impersonation and fraudulent voting, providing an additional layer of verification in the voting process.

II. NEED OF THE STUDY

Evolution of India's Voting System: During the initial years of democratic voting, India used a manual paper ballot system. People had to go to polling stations, where their identities were ascertained prior to being issued a ballot paper. They would then secretly indicate their desired candidate and drop the ballot in an enclosed box. To avoid double voting, fingers of voters were marked with ink that could not be erased. Although this system provided vote records and recorded turnout, it was manpower-intensive, error-prone, time-consuming, and vulnerable to tampering and fraud.

To overcome these deficits, Electronic Voting Machines (EVMs) came as a technological solution. EVMs replaced paper ballots, made vote casting and counting quicker and more efficient, and enhanced efficiency, especially in far-flung localities. But initial EVMs were criticized on issues of security risks, transparency deficits, and inability to provide verifiable audit trails. Fears of possible tampering necessitated the invention of the Voter Verified Paper Audit Trail (VVPAT), enabling voters to check their choices through printed receipts. Although EVMs greatly enhanced the electoral process, trust, verifiability, and security issues still exist. Continuous innovation is required to develop a system that is not only efficient but also completely transparent, secure, and inclusive.

III. SYSTEM-ARCHITECTURE

The proposed computerized Electronic Voting Machine (EVM) is developed using Verilog HDL to ensure a secure, transparent, and efficient election process. The system begins by identifying the total number of voters and candidates, followed by assigning a Voting Enable signal to each eligible participant for authentication. A voter switch input mechanism ensures that only authorized voters can cast their votes, preventing duplicate or unauthorized entries.

During the voting phase, each vote is recorded in the respective candidate's register, guaranteeing accurate and tamper-proof counting. Once all votes are submitted, a verification module validates the results to detect and correct potential errors instantly. This structured and automated approach enhances reliability, eliminates manual intervention, and ensures fair and error-free election outcomes.

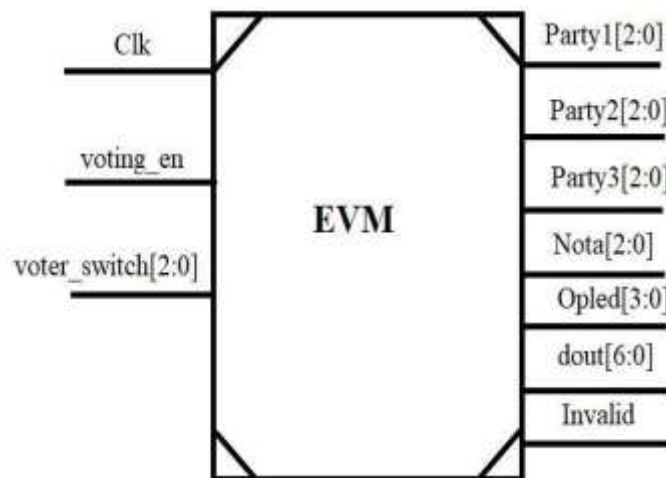


Fig1: EVM Schematic

The figure illustrates the **block diagram of the Electronic Voting Machine (EVM)** implemented using Verilog HDL. It represents the primary input and output ports of the EVM system and their interconnections.

Inputs:

- Clk: The clock signal that synchronizes all operations within the EVM.
- voting_en: The voting enable signal that activates the voting process, allowing registered voters to cast their votes.
- voter_switch[2:0]: The voter input switches used to select a particular candidate or party.
- Outputs:
- Party1[2:0], Party2[2:0], Party3[2:0]: These indicate the total votes registered for each party.
- Nota[2:0]: Represents the "None of the Above" (NOTA) option votes.
- OpLED[3:0]: The output LEDs that visually display the active voting or counting status.
- dout[6:0]: A seven-segment display output showing the total number of votes or results.
- Invalid: This output is triggered if an invalid voting attempt or signal is detected.

Overall, this block diagram defines the **functional interface** of the FPGA-based EVM system, ensuring secure and reliable vote processing.

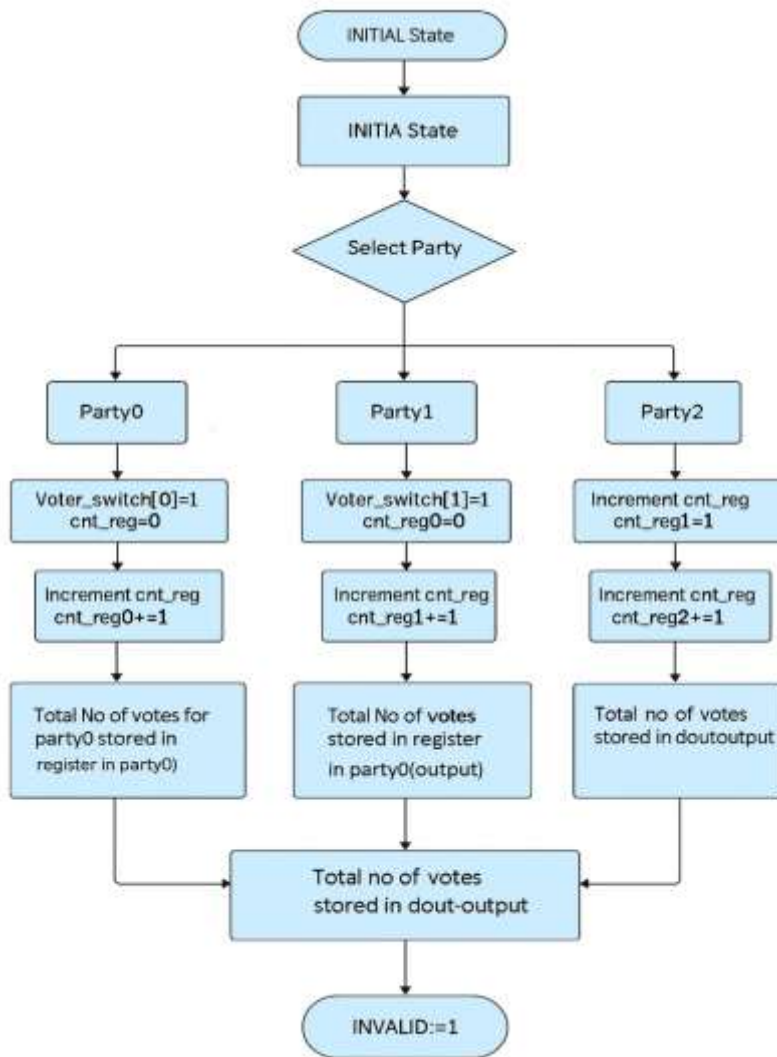


Fig.2 Flow Chart of EVM

From figure2, the flowchart illustrates the **voting workflow of a Verilog-based Electronic Voting Machine (EVM)**. It begins with system initialization, followed by a voter selecting one of three parties. When a valid switch is pressed, the corresponding party's vote counter increments, and an LED indicator confirms the vote. Each party's total votes are stored in separate registers, and the overall total is recorded in the output register. If any invalid input is detected, an error flag ($INVALID = 1$) is triggered. The design ensures **accurate vote counting, input validation, and secure operation** throughout the election process.

IV. RESULTS AND DISCUSSIONS

The figure 3 illustrates the **behavioral simulation waveform** of the proposed **Verilog-based Electronic Voting Machine (EVM)** using Xilinx ISE. The signals include clk (clock pulse), $voting_en$ (voting enable), $voter_switch[2:0]$ (party selection inputs), $person[11:0]$ (voter identification), and output registers for each party (party1, party2, party3). As the clock cycles progress, the voter switches activate sequentially, and the corresponding party counters increment correctly. The $opled[3:0]$ signal glows to confirm a valid vote, while the $invalid$ signal remains low, indicating no unauthorized input. The waveform also shows cumulative vote counts being updated in real time for each party. The simulation confirms that the system accurately registers votes, prevents multiple voting, and maintains synchronization between input and output signals. This demonstrates the correct functional behavior and timing efficiency of the designed EVM architecture on the FPGA platform.

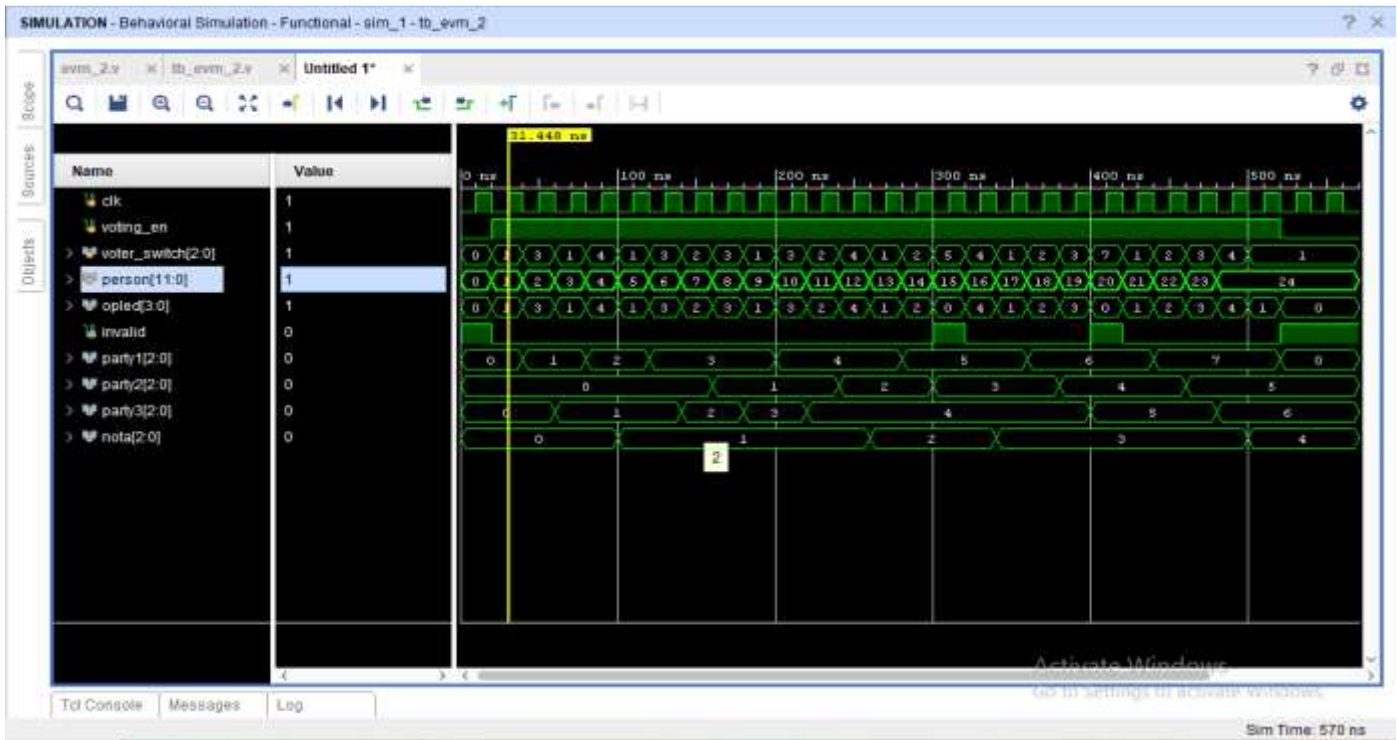


Fig3: output waveform when voted casted for party1

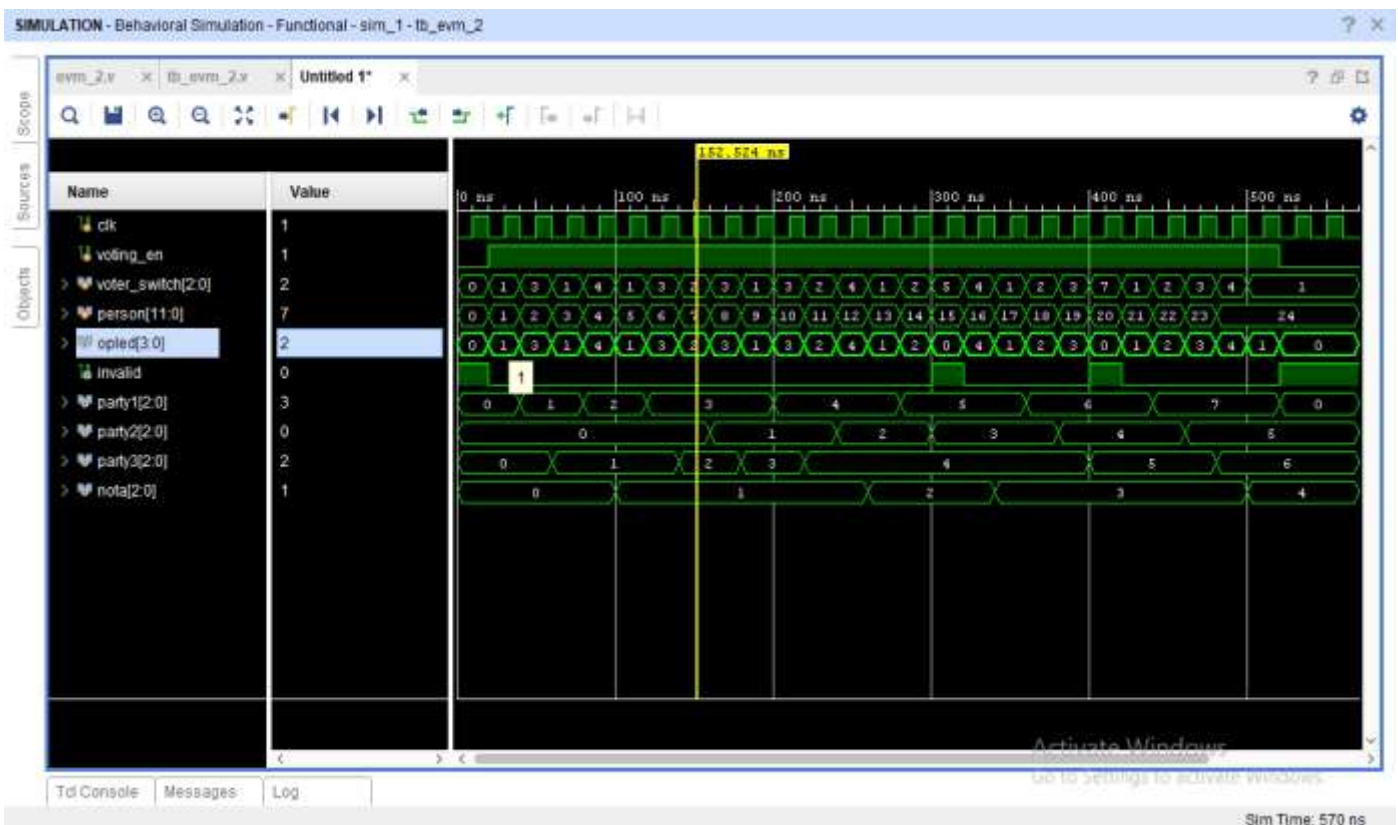


Fig4: output waveform when voted casted for party2

The figure 4 illustrates the **simulation waveform** of the Verilog-based **Electronic Voting Machine (EVM)**, showing signal interactions during voting. The clock (clk) synchronizes all operations, while voting_en activates the voting process. The voter_switch inputs represent party selections, and opled confirms each valid vote through LED indication. The registers party1, party2, and party3 increment correctly as votes are cast, while the invalid signal remains low, indicating no unauthorized input. Overall, the simulation verifies that the EVM accurately counts votes, responds to valid inputs, and maintains proper synchronization and functionality.

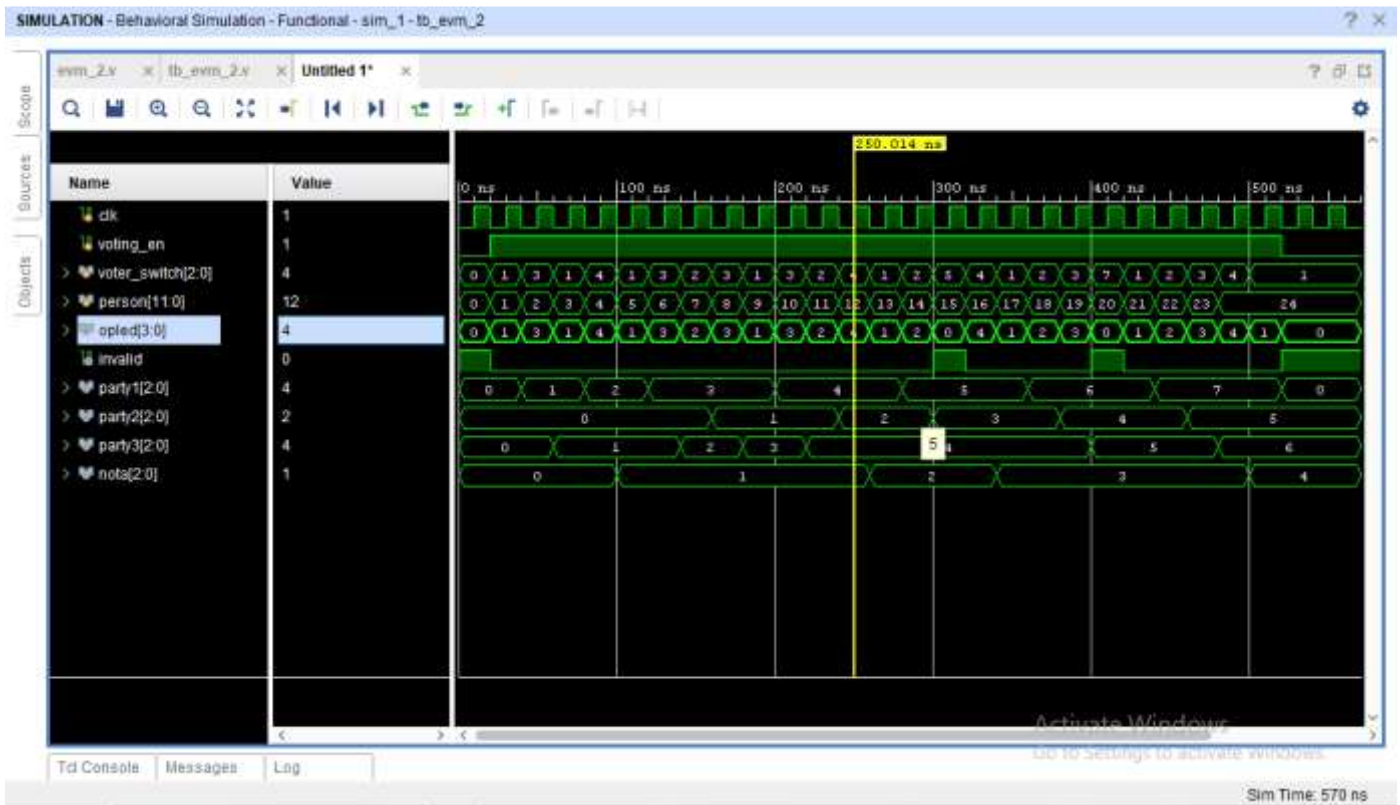


Fig5: output waveform when voted casted for Nota

The figure 5 displays the behavioral simulation waveform of the Verilog-based Electronic Voting Machine (EVM), demonstrating the functional behavior of the voting process in real time. The `clk` signal provides the timing synchronization for the system, while `voting_en` activates the voting sequence. The `voter_switch[2:0]` input represents the voter's party selection, and in this instance, multiple switches are activated sequentially to simulate votes for different parties. The `person[11:0]` signal identifies individual voters. When a valid vote is cast, the `opled[3:0]` output glows, confirming successful vote registration. The `party1`, `party2`, and `party3` registers increment accordingly, reflecting accurate vote counting for each party. The `invalid` signal remains at logic low (0), confirming that no unauthorized or duplicate input occurred during the voting process. This waveform validates the correct operation, synchronization, and secure vote recording of the EVM implemented using Verilog HDL on the FPGA.

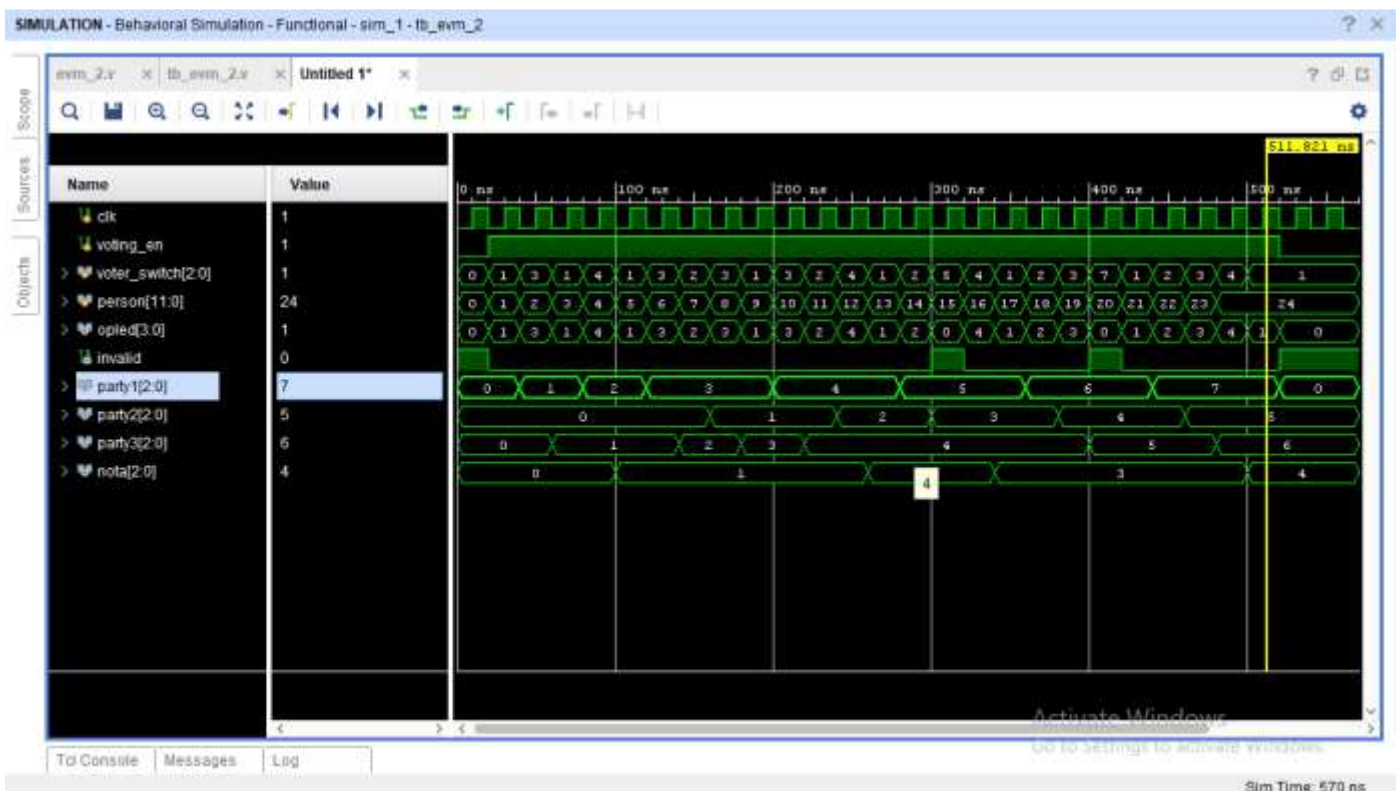


Fig6: output waveform when overall votes casted

The figure 6 illustrates the **behavioral simulation waveform** of the **Verilog-based Electronic Voting Machine (EVM)** implemented on FPGA, showing the system's signal behavior over time. The `clk` signal represents the system clock that

synchronizes all operations. The voting_en signal enables the voting process, allowing input through voter_switch[2:0], which specifies the selected party. The person[11:0] signal indicates the unique voter identification, ensuring that each person can vote only once. As each valid vote is cast, the opled[3:0] output activates, confirming a successful vote, while the invalid signal remains at logic '0', indicating that no invalid or duplicate inputs occurred. The party1, party2, **and** party3 registers update dynamically as votes are recorded for the corresponding parties. By the end of the simulation, the waveform confirms accurate vote counting and secure operation, demonstrating that the EVM design effectively synchronizes inputs, validates voter eligibility, and reliably stores the election results.

V. CONCLUSION

The Xilinx-based Electronic Voting Machine (EVM) effectively meets the essential requirements of the election process. It begins with enrolling the total number of voters and contestants, followed by allowing each voter to securely cast a vote for the party of their choice. These votes are validated to ensure correctness and reliability. In the final stage, the system compares all valid votes polled for different parties and identifies the winner. A key feature of the system is its authentication process before voting, which enhances transparency and security. The design is efficient and can be implemented on any FPGA board with ease. Future enhancements include integrating biometric security using fingerprint authentication and individual voter cards to further secure the voting process. Additionally, the system can be adapted for PRSTV (Proportional Representation Single Transferable Vote) elections, which involve casting multiple votes, as seen in elections for the President, Vice President, and Vidhana Parishad.

REFERENCES

- [1] K. Czajkowski, S. Fitzgerald, I. Foster, and C. Kesselman, "Grid information services for distributed resource sharing," in *Proc. 10th IEEE Int. Symp. High Performance Distributed Computing (HPDC)*, New York, USA, pp. 181–184, 2001.
- [2] I. Foster, C. Kesselman, J. Nick, and S. Tuecke, "The physiology of the grid: An open grid services architecture for distributed systems integration," *Global Grid Forum*, Technical Report, 2002.
- [3] P. May, H. C. Ehrlich, and T. Steinke, "ZIB structure prediction pipeline: Composing a complex biological workflow through web services," in *Euro-Par 2006 Parallel Processing*, W. E. Nagel, W. V. Walter, and W. Lehner, Eds. *Lecture Notes in Computer Science (LNCS)*, vol. 4128, Springer, Heidelberg, pp. 1148–1158, 2006.
- [4] N. S. N. Lakshmi Pathi Raju, A. Pravin, N. S. Murthy Sharma, and S. S. Kiran, "A novel proposal on implementation of polling percentage improvement system through embedded-based integration of electronic voting machine and other methodologies," *International Journal of Emerging Technologies and Applications in Engineering, Technology and Sciences (IJETA-ETS)*, vol. 5, no. 2, pp. 1–5, Jul.–Dec. 2012.
- [5] K. S. Gurucharan, B. Kiranmai, S. S. Kiran, and M. R. Kumar, "Xilinx based electronic voting machine," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 1, pp. 1–5, Oct. 2019.
- [6] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 323–341, 2020.
- [7] X. Lin, "College student employment data platform based on FPGA and machine learning," *Microprocessors and Microsystems*, vol. 79, pp. 103–120, 2020.
- [8] S. Vemula, R. M. R. Kovvur, and D. Marneni, "Secure e-voting system implementation using CryptDB," *SN Computer Science*, vol. 2, no. 3, pp. 1–6, 2021.