Capstone Project Proposal Report
(Individual Report)

Instructions:

This form is to be completed by each student doing Project registration to fulfill their senior design or capstone requirement. It must be completed and submitted to your Guide. Each student must complete this form individually.

This report is to be completed during the starting of the semester, while the project description report will be completed during end of the semester.

Guide Approval (initials/date):		14-08-2024

CAP4001– Capstone Project Proposal Report

Student Name	Tarun Gampala
Student Register Number	21BEC7115
Programme	BTech
Semester/Year	4th year 7th Semester
Guide(s)	Prof Sucharitha Jackson
Project Title	VLSI Architecture Design of Advanced Encryption Standard Algorithms

Team Composition: Provide the information below for each member of the **project team**. Include **all** project team members, not just those in your discipline or those enrolled for Capstone project. Please also include yourself!

Reg. No	**Name**	**Major**	**Specialization**
21BEC7115	Tarun Gampala	ECE	Spec VLSI
21BEC7009	M N S Manoj	ECE	Spec VLSI
21BEC7061	N Sirisha Kumari	ECE	Minor in Data Analytics

Project and Task Description: The goal of this project is to design and implement the AES-128 encryption algorithm in Verilog for FPGA or ASIC applications. AES (Advanced Encryption Standard) is a widely used symmetric encryption algorithm that operates on 128-bit data blocks and uses a 128-bit key. This project will involve creating Verilog modules for the AES components and integrating them into a complete AES encryption system.

Objectives and Tasks:

1. **Understand AES-128 Algorithm:** Gain a thorough understanding of AES-128 encryption, including key expansion, encryption rounds, and the specific operations performed in each round.
2. **Design Verilog Modules**: Implement the key components of AES-128 in Verilog, including SubBytes, ShiftRows, MixColumns, AddRoundKey, and Key Expansion.
3. **Integrate Modules:** Combine the individual modules into a complete AES-128 encryption system.
4. **Simulate and Verify**: Develop testbenches to simulate and verify the functionality of the AES implementation. Ensure that the design meets the AES-128 specifications.
5. **Optimize**: Optimize the design for performance, area, and power consumption as needed.

Outcome Matrix: Describe your plan to demonstrate each of the outcomes below.

Outcomes:	**Plan for demonstrating outcome:**
a) an ability to apply knowledge of mathematics, science, and engineering	Implementing AES-128 in Verilog requires applying mathematical principles such as finite field arithmetic and matrix operations, which are crucial for cryptographic functions and key expansion. It also demands a solid understanding of computer science concepts, including algorithm design and data structures, to accurately model the encryption process. Additionally, knowledge of digital logic design and hardware optimization from electrical engineering is essential to effectively translate the AES algorithm into a hardware description, ensuring efficient and accurate implementation on FPGA or ASIC platforms.
c) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability	When simulating an AES-128 encryption system in Verilog, the design must balance constraints to meet desired needs. Economically, the simulation should be efficient, minimizing computational resources and time. Environmentally, while simulation itself has minimal impact, optimizing the design can lead to more efficient hardware implementations. Socially, the simulation should ensure that the encryption process meets privacy and security standards. Politically, the simulation must adhere to relevant regulations and standards for data protection. Ethically, the design should be used responsibly, avoiding potential misuse. Health and safety considerations are less relevant in simulation but still involve ensuring that the simulated system operates correctly and reliably.
d) an ability to function on multidisciplinary teams	In simulating an AES-128 encryption system using Verilog, the ability to identify, formulate, and solve engineering problems involves several key steps. Identify: Recognize challenges such as ensuring correct implementation of AES operations, managing timing constraints, and verifying accuracy of encryption results. Formulate: Develop a clear approach to address these challenges by designing comprehensive testbenches, defining simulation parameters, and specifying expected outputs for each AES operation. Solve: Implement the Verilog code, run simulations to test functionality, debug issues as they arise, and refine the design based on test results to ensure that the encryption system performs as specified and meets all requirements. This iterative process ensures a robust and accurate simulation of the AES-128 algorithm.
e) an ability to identify, formulate, and solve engineering problems	To simulate an AES-128 encryption system in Verilog, the ability to identify, formulate, and solve engineering problems involves first recognizing issues such as incorrect AES operations or timing mismatches. Formulate a structured approach by creating detailed testbenches, defining simulation scenarios, and setting expected results for each AES function. Solve these problems by implementing the Verilog code, running simulations to detect and correct errors, and iterating on the design to ensure it meets all functional and performance requirements. This process ensures a robust and accurate simulation of the AES-128 algorithm.
g) an ability to communicate effectively	Effectively communicating in the context of simulating an AES-128 encryption system in Verilog involves clearly articulating design goals, explaining the simulation methodology, and presenting results in a comprehensible manner. This includes documenting the design process, specifying the implementation details of each Verilog module, and summarizing test outcomes and any issues encountered. Additionally, providing clear and concise reports, presentations, or discussions helps stakeholders understand the system's functionality, performance, and any necessary improvements, ensuring that all team members and users are aligned and informed.
k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice	For implementing AES in Verilog, leveraging modern engineering tools and techniques is crucial. This involves utilizing hardware description languages like Verilog to accurately model and design the AES-128 encryption algorithm, employing simulation tools such as ModelSim or Vivado to test and validate the design thoroughly. Additionally, using synthesis tools for optimizing the Verilog code ensures that the design is efficient in terms of area, speed, and power consumption. Skills in digital logic design, including understanding finite

	field arithmetic and encryption algorithms, are essential. Keeping abreast of the latest industry practices and tools allows for the effective application of these techniques to achieve a robust and high-performance AES implementation.

Realistic Constraints:

When designing an AES-128 encryption system in Verilog, several realistic constraints must be considered:

1. **Economic Constraints**: Ensure the design is cost-effective by optimizing hardware usage and minimizing resource consumption. This involves balancing performance with cost to keep implementation within budget.
2. **Performance Constraints**: The design must meet specific performance requirements, such as processing speed and throughput, to ensure it can handle encryption tasks efficiently.
3. **Resource Constraints**: Limited FPGA or ASIC resources, such as logic gates, memory, and I/O pins, must be managed to fit the AES design within available hardware constraints.
4. **Power Consumption**: The design should be optimized for low power consumption to extend battery life in portable devices and reduce energy costs in larger systems.
5. **Timing Constraints**: The system must meet timing requirements to ensure that encryption and decryption processes occur within acceptable time frames without introducing delays or errors.
6. **Scalability**: The design should be adaptable to future enhancements or changes in encryption standards without requiring a complete redesign.
7. **Environmental Constraints**: Considerations such as temperature and voltage ranges are essential to ensure the design operates reliably in its intended environment.
8. **Compliance and Security**: The design must adhere to industry standards and regulations for cryptographic security and data protection to ensure the encryption is effective and legally compliant.
9. **Usability and Integration**: The AES system should be designed for easy integration with existing systems and user-friendly interfaces to ensure practical applicability.

Engineering Standards:

When designing an AES-128 encryption system in Verilog, adherence to engineering standards ensures the robustness, reliability, and effectiveness of the implementation. Key engineering standards to consider include:

1. **Cryptographic Standards**: Follow established cryptographic standards such as FIPS 197 (which specifies AES) to ensure that the encryption implementation is secure and compliant with recognized practices.
2. **Design Methodologies**: Adhere to digital design methodologies, including modular design principles, to create a well-structured and maintainable Verilog codebase. This involves using standard practices for designing and documenting digital systems.
3. **Simulation and Verification Standards**: Employ standard practices for simulation and verification, such as writing comprehensive testbenches, performing functional and timing simulations, and ensuring that the design meets all specified requirements.
4. **Hardware Description Language (HDL) Standards**: Use Verilog language constructs and coding practices that comply with IEEE standards (e.g., IEEE 1364 for Verilog) to

ensure code portability, readability, and compatibility with synthesis and simulation tools.

5. **Performance Optimization**: Follow best practices for optimizing digital designs, including techniques for minimizing area, power, and delay, to ensure that the AES implementation performs efficiently within hardware constraints.
6. **Documentation Standards**: Maintain thorough documentation that includes design specifications, implementation details, test plans, and results. This documentation should follow standard practices to facilitate understanding, maintenance, and verification by others.
7. **Safety and Reliability Standards**: Ensure the design meets safety and reliability standards to prevent faults and ensure correct operation under all specified conditions. This includes designing for fault tolerance and performing reliability testing.
8. **Compliance with Regulatory Requirements**: Adhere to any relevant regulatory and industry-specific standards that apply to encryption systems, such as data protection regulations and export controls on cryptographic technology.

By adhering to these engineering standards, the AES-128 design will be robust, secure, and suitable for practical deployment.