FPGA based RTL Design and Verification of AES Algorithm

Abstract

The project aims to design and verify the Advanced Encryption Standard (AES) algorithm using Field-Programmable Gate Array (FPGA) technology design flow approach. This involves two primary phases: Phase-1 focuses on understanding AES specifications, developing Register Transfer Level (RTL) using Verilog HDL, ensuring functional correctness through simulation, and performing FPGA-based synthesis using AMD's Vivado tool. Phase-2 encompasses backend tasks such as floorplanning, placement, clock tree synthesis, routing, and the generation of a bitstream file using AMD's Vivado tool. This project not only deepens our understanding of AES but also showcases the complete design flow application of FPGA technology in encryption.

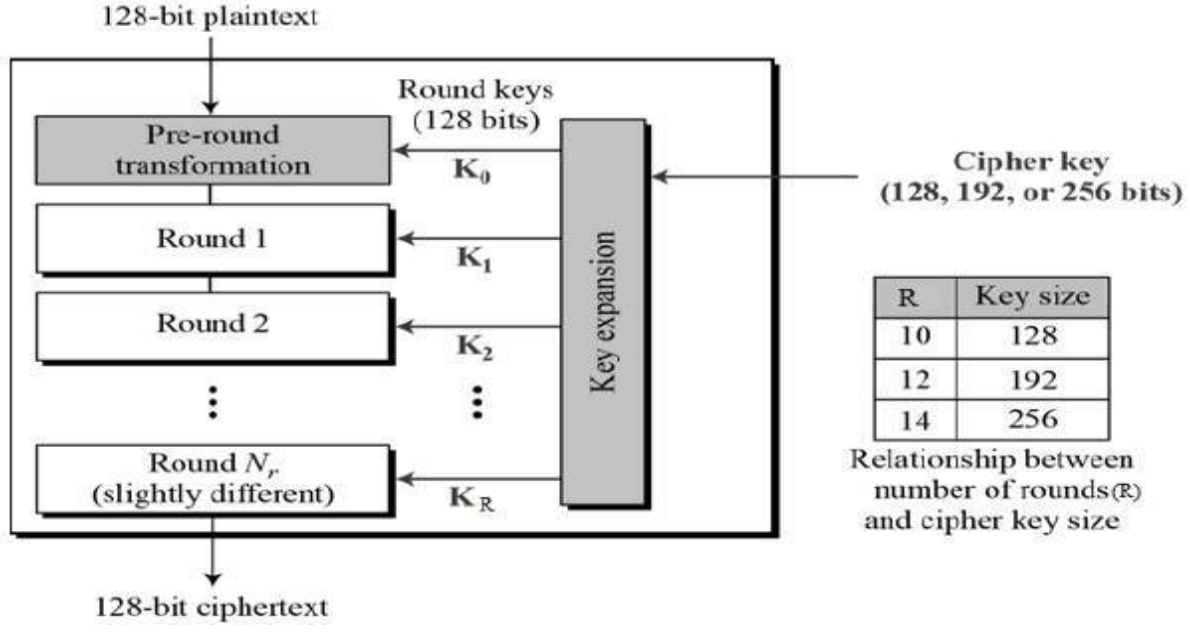
Introduction

In an era of increasing data security concerns, encryption plays a pivotal role in safeguarding sensitive information. The AES algorithm, a symmetric key encryption standard, has gained prominence due to its robustness and efficiency. Leveraging FPGA technology for AES implementation offers flexibility and customization, making it an ideal platform for encryption applications.

Problem Statement

The project addresses the need for a reliable and efficient implementation of the AES algorithm on FPGA. While software-based implementations are widely used, they may not always meet the stringent performance requirements of real-time applications. FPGA-based solutions provide the advantage of parallelism and hardware acceleration, allowing for faster encryption and decryption processes.

Block Diagram:



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Phase 1: Understanding AES Algorithm and RTL Development

1: Understanding AES Algorithm and its Specifications

This initial phase involves an in-depth study of the AES algorithm, comprehending its underlying mathematical operations, key expansion, and encryption/decryption processes. Understanding the algorithm's specifications lays the foundation for subsequent RTL development.

2: Developing RTL using Verilog HDL

With a clear grasp of AES, the next step is the development of Register Transfer Level (RTL) using Verilog HDL. This phase involves translating the algorithmic steps into hardware components, including the substitution-permutation network (SPN), key expansion, and other crucial modules.

3: Ensuring RTL Correctness through Functional Simulation

Functional simulation serves as a critical validation step before moving to synthesis. It involves testing the RTL design against various test vectors to ensure it performs as expected under different scenarios. This phase helps uncover any logic errors or discrepancies in the design.

4: Performing FPGA-based Synthesis Flow

The final task of Phase 1 involves synthesizing the RTL code for FPGA implementation. This process translates the high-level RTL description into a netlist that can be mapped onto the FPGA's logic elements. AMD's Vivado tool will be employed to carry out this synthesis.

Phase 2: Backend Implementation and Bitstream Generation

1: Floorplanning, Placement, and Clock Tree Synthesis

Phase 2 focuses on the backend implementation of the design. This involves tasks such as floorplanning, which determines the placement of critical components, placement, which assigns logic elements to specific locations, and clock tree synthesis to ensure proper clock distribution.

2: Routing and Bitstream Generation

Routing involves establishing connections between logic elements, ensuring signal integrity and performance. Subsequently, the generation of the bitstream file is the final step, producing a file that can be loaded onto the FPGA for functional testing.

Conclusion

This project embarks on the ambitious journey of implementing the AES algorithm on FPGA, combining theoretical knowledge with hands-on practical application. Phase 1 establishes a robust RTL design, while Phase 2 delves into the intricacies of backend implementation. Through this project, we aim to not only enhance our understanding of AES but also demonstrate the potential of FPGA technology in encryption applications.