A DESIGN AND IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD ALGORITHM AES-128bits ON FPGA XILINX KIT

***Nguyen My Qui*[1] *Nguyen Duy Manh Thi*[2]**
[1]Department of Electronic and Computer Engineering
National Taiwan University of Science and Technology
[2]Faculty of Electronics and Telecommunications
University of Science, VNU-HCM
m10702809@mail.ntust.edu.tw, ndmthi@fetel.hcmus.edu.vn

Abstract

Advanced Encryption Standard (AES) is one of the most popular cryptographic algorithms using variable-length symmetric keys for block encryption and decryption. FPGA-based AES cryptographic design combines the high-security advantages of the AES standard with the outstanding reprogrammability and parallel processing capability of FPGA technology. This paper introduces the mathematic principles of the encryption/decryption process, and the logical structure of the 128-bit AES algorithm. The whole architecture is then designed using Verilog Hardware Description Language (HDL) and synthesized on a field-programmable gate array (FPGA) Virtex-5 xc5vlx50-2ff676 platform. The frequency of the encryption module achieves up to 206.083MHz with 1.65Gbps throughput, and the decryption module operates at 202.655MHz frequency and 1.0Gbps throughput.

Keywords: advanced encryption standard (AES), field-programmable gate arrays (FPGA), cryptography, Verilog.

XÂY DỰNG VÀ THỰC HIỆN THUẬT TOÁN MÃ HÓA NÂNG CAO AES-128bits (SINGLE-CHIP CRYPTO) TRÊN FPGA XILINX KIT

***Nguyễn Mỹ Quí*[1] *Nguyễn Duy Mạnh Thi*[2]**
[1]Khoa Kỹ thuật Điện tử và Máy tính
Đại học Khoa học và Công nghệ Quốc gia Đài loan
[2]Khoa Điện Tử Viễn Thông
Trường Đại học Khoa học Tự Nhiên, ĐHQG-HCM
m10702809@mail.ntust.edu.tw, ndmthi@fetel.hcmus.edu.vn

Tóm tắt

Tiêu chuẩn mã hóa nâng cao Advanced Encryption Standard (AES) là một trong những thuật toán mã hóa phổ biến nhất sử dụng khóa mã đối xứng để mã hóa và giải mã khối với các độ dài khóa đa dạng. Thiết kế chip mã hóa AES trên nền công nghệ FPGA là giải pháp kết hợp ưu điểm bảo mật cao của chuẩn AES với khả năng tái lập trình vượt trội và khả năng xử lý song song của công nghệ FPGA. Bài báo này giới thiệu nguyên tắc toán học, quá trình mã hóa và giải mã, và kiến trúc logic của thuật toán AES 128 bits. Sau đó toàn bộ kiến trúc được thiết kế sử dụng ngôn ngữ mô tả phần cứng Verilog (HDL) và tổng hợp trên kit FPGA Xilinx Virtex-5 XC5VLX50-2FF676. Tần số của khối module mã hóa đạt được lên đến 206,083 Mhz với thông lượng 1,65Gbps và module giải mã tương ứng hoạt động ở tần số là 202,655 MHz và thông lượng 1,0Gbps.

Từ khóa: advanced encryption standard (AES), field-programmable gate arrays (FPGA), cryptography, Verilog.