**AES IP CORE SPECIFICATION**

Contents

[I. THIẾT KẾ KHỐI XỬ LÝ MẬT MÃ AES-128 2](#_Toc150010778)

[1. Tổng quan thiết kế 2](#_Toc150010779)

[2. Yêu cầu chức năng 2](#_Toc150010780)

[3. Sơ đồ khối 2](#_Toc150010781)

[3.1. Sơ đồ khối top module 2](#_Toc150010782)

[3.2. Sơ đồ khối sub module 3](#_Toc150010783)

# THIẾT KẾ KHỐI XỬ LÝ MẬT MÃ AES-128

## Tổng quan thiết kế

Xây dựng lõi IP xử lý mật mã AES-128 hoạt động ở cả 2 chức năng mã hoá, giải mã. Ở chế độ mã hoá, đầu vào bao gồm bản rõ (Plain Text) và Khoá (Cipher Key) có độ dài 128-bit, đầu ra thu được bản mã (Cipher Text) có độ dài tương ứng 128-bit, tương tự với chế độ giải mã.

## Yêu cầu chức năng

* Thiết kế lõi IP xử lý mật mã AES-128 (Advance Encryption Standard chuẩn 128-bit) ở cả 2 chức năng Mã hoá và Giải mã.
* Từ bản đặc tả thiết kế, sử dụng ngôn ngữ mô tả phần cứng SystemVerilog để lập trình, mô phỏng và kiểm thử chức năng.
* Triển khai thiết kế trên nền tảng FPGA, sử dụng kit Altera DE2-70, giao tiếp với máy tính, gửi và nhận thông tin mã hoá, giải mã.
* Yêu cầu khối mạch hoạt động đúng chức năng, đáp ứng về mặt thời gian, độ chính xác, ưu tiên thiết kế tối ưu hoá về mặt tài nguyên.

## Sơ đồ khối

### 3.1. Sơ đồ khối top module

A white background with black text

Description automatically generated

*Hình 3.1 Sơ đồ khối AES\_Encrypt\_Top\_Module*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên tín hiệu** | **Số bit** | **Hướng tín hiệu** | **Mô tả** |
| clk | 1 | Đầu vào | Xung đồng hồ |
| reset\_n | 1 | Đầu vào | Tín hiệu reset, tích cực mức thấp |
| plain\_text | 128 | Đầu vào | Bản rõ đầu vào, 128-bit dữ liệu |
| cipher\_key | 128 | Đầu vào | Khoá đầu vào, 128-bit dữ liệu |
| cipher\_new\_en | 1 | Đầu vào | Tín hiệu kích hoạt bộ giải mã hoạt động, tích cực 1 chu kỳ xung đồng hồ |
| cipher\_text | 128 | Đầu ra | Bản mã đầu ra, 128-bit dữ liệu |
| cipher\_finish | 1 | Đầu ra | Cờ báo hiệu kết thúc quá trình mã hoá, tích cực mức cao |

*Hình 3.2 Bảng mô tả các chân tín hiệu khối top module*

### Sơ đồ khối sub module

#### Khối AES\_Encrypt\_Key\_Expand

A white background with black text

Description automatically generated

*Hình 3.2.1 Sơ đồ khối AES\_Encrypt\_Key\_Expand*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên tín hiệu** | **Số bit** | **Hướng tín hiệu** | **Mô tả** |
| clk | 1 | Đầu vào | Xung đồng hồ |
| reset\_n | 1 | Đầu vào | Tín hiệu reset, tích cực mức thấp |
| cipher\_key | 128 | Đầu vào | Khoá đầu vào, 128-bit dữ liệu |
| cipher\_new\_en | 1 | Đầu vào | Tín hiệu kích hoạt bộ giải mã hoạt động, tích cực 1 chu kỳ xung đồng hồ |
| round\_num | 3 | Đầu vào | Số vòng mã hoá hiện tại, 3-bit dữ liệu |
| round\_key\_out | 128 | Đầu ra | Khoá vòng mở rộng, 128-bit dữ liệu |

*Bảng 3.2.1 Bảng mô tả chân tín hiệu khối AES\_Encrypt\_Key\_Expand*

*A diagram of a computer

Description automatically generated*

*Hình 3.1.2 Kiến trúc khối AES\_Encrypt\_Key\_Expand*

#### Khối AES\_Encrypt\_Core

A white background with black text

Description automatically generated

*Hình 3.2.2 Sơ đồ khối AES\_Encrypt\_Core*

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên tín hiệu** | **Số bit** | **Hướng tín hiệu** | **Mô tả** |
| clk | 1 | Đầu vào | Xung đồng hồ |
| reset\_n | 1 | Đầu vào | Tín hiệu reset, tích cực mức thấp |
| plain\_text | 128 | Đầu vào | Bản rõ đầu vào, 128-bit dữ liệu |
| cipher\_key | 128 | Đầu vào | Khoá đầu vào, 128-bit dữ liệu |
| round\_key | 128 | Đầu vào | Khoá đầu vào mỗi vòng giải mã, 128-bit dữ liệu |
| cipher\_new\_en | 1 | Đầu vào | Cờ kích hoạt bộ giải mã hoạt động, tích cực 1 chu kỳ xung clock |
| round\_key\_en | 1 | Đầu ra | Cờ báo hiệu bộ mở rộng khoá hoạt động |
| cipher\_finish | 1 | Đầu ra | Cờ báo hiệu kết thúc quá trình mã hoá |
| round\_num | 3 | Đầu ra | Số vòng mã hoá hiện tại, 3-bit dữ liệu |
| cipher\_text | 128 | Đầu ra | Bản mã đầu ra, 128-bit dữ liệu |

*Bảng 3.2.2 Bảng mô tả các chân tín hiệu khối AES\_Encrypt\_Core*

*A diagram of a block diagram

Description automatically generated*