AWS\_aes解密使用说明书

# 程序功能

## 1.1概述

本设计主要功能是ESP32通过QSPI串行通信接口，将128bit加密数据发送到FPGA中，并通过aes解密算法还原成原来未加密的8bit传感器输入数据，最后将解密的数据通过IO口输出出来。

前期处理是ESP32加载AWS云端已经由发送者发送好的128bit加密数据。这部分程序在ESP32上实现，本说明未加入详细叙述，请参考ESP32部分说明。

备注:绿色部分是本说明文件外的部分,程序未在此文档下,黑色部分为FPGA加密部分。

## 1.2项目总体架构

AWS云

AWS\_aes

加密模块

8bitAD数据

data

ESP32

128bit加密的AD数据

QSPI通信协议

FPGA

发送板卡

128bit加密的AD数据

ESP32

QSPI通信协议

AWS云

AWS\_aes

解密模块

8bitAD数据

data

FPGA

接收板卡

备注:下图绿色部分是本说明文件外的部分,程序未在此文档下,黑色部分为FPGA加密部

# 二、解密程序架构

## 1整体架构图

key\_bus[3:0]

AWS\_aes\_Inverse

sclk

rst\_n

raw\_data [7:0]

DONE

led\_en

I\_qspi\_cs

qspi\_data[3:0]

I\_qspi\_clk

## 2.架构使用说明

AWS\_aes\_Inverse是一个秘钥可变动的AES解密算法，秘钥通过4位拨码开关加载，可随时变更；

加载秘钥后密钥数据加载到解密模块形成解密扩展密钥，密钥加载完毕后输出kld信号允许解密数据加载。

加密数据通过ESP32的QSPI信道传输到RAM中，然后传输到解密模块完成解密并输出相关的解密后的数据。

加密数据存储到FPGA内部的RAM中，存储地址为8'b0000\_0010到8'b0001\_0001；

LED灯将显示解密后的数据，根据阈值大小点亮或者熄灭，主要做测试使用。

## 3.引脚说明

sclk：系统输入时钟100MHz；

rst\_n：复位引脚；

key\_bus: 4位可变秘钥输入端口，本设计接入四位拨码开关接；

I\_qspi\_cs：qspi片选信号；

I\_qspi\_clk：qspi时钟信号；

qspi\_data[3:0]：qspi数据线，在设计中是分开的四根线；

raw\_data：8位解密后的原始数据输入端口；

DONE:解密完成使能端口；

led\_en：led灯使能端口，主要做测试使用，当模拟量输入大于8'b0001\_1111时，绿色led灯点亮，当模拟量输入小于上述阈值时led灯灭。

# 二、内部架构说明

## 1.内部架构图

rst\_n

sclk

data\_ compression

key\_

128test

4bit转128bit

aes\_inv\_cipher\_top

aes解密模块

key\_bus[3:0]

K1

K2

K3

K4

DONE

test\_out

en\_kld

done

key\_128

raw\_data[7:0]

en

QSPI\_

slave

Id

kdone

aes\_data[127:0]

I\_qspi\_clk

I\_qspi\_cs

qspi\_data[3:0]

ESP

32

LED\_

control

ram\_count

add8[7:0]

led\_en

LED

ram\_data[7:0]

RAM

data8[7:0]

**AWS\_aes\_Inverse**

## 2.架构详细说明

复位键低电平复位后，key\_128test模块开始加载4位秘钥并转化成128位的AES算法秘钥，秘钥转化完成后同时输出使能信号和128位算法秘钥；秘钥是能后aes解密模块（aes\_inv\_cipher\_top）输出kdone信号标志密钥加载完毕，此时允许解密数据加载到aes解密模块；

ESP32通过QSPI通信协议，将14\*8bit数据写入RAM，ram\_count将8bit数据链接成128bit的AES解密数据，并在kdone使能后，使能Id信号和输出128bit解密数据到aes解密模块，；

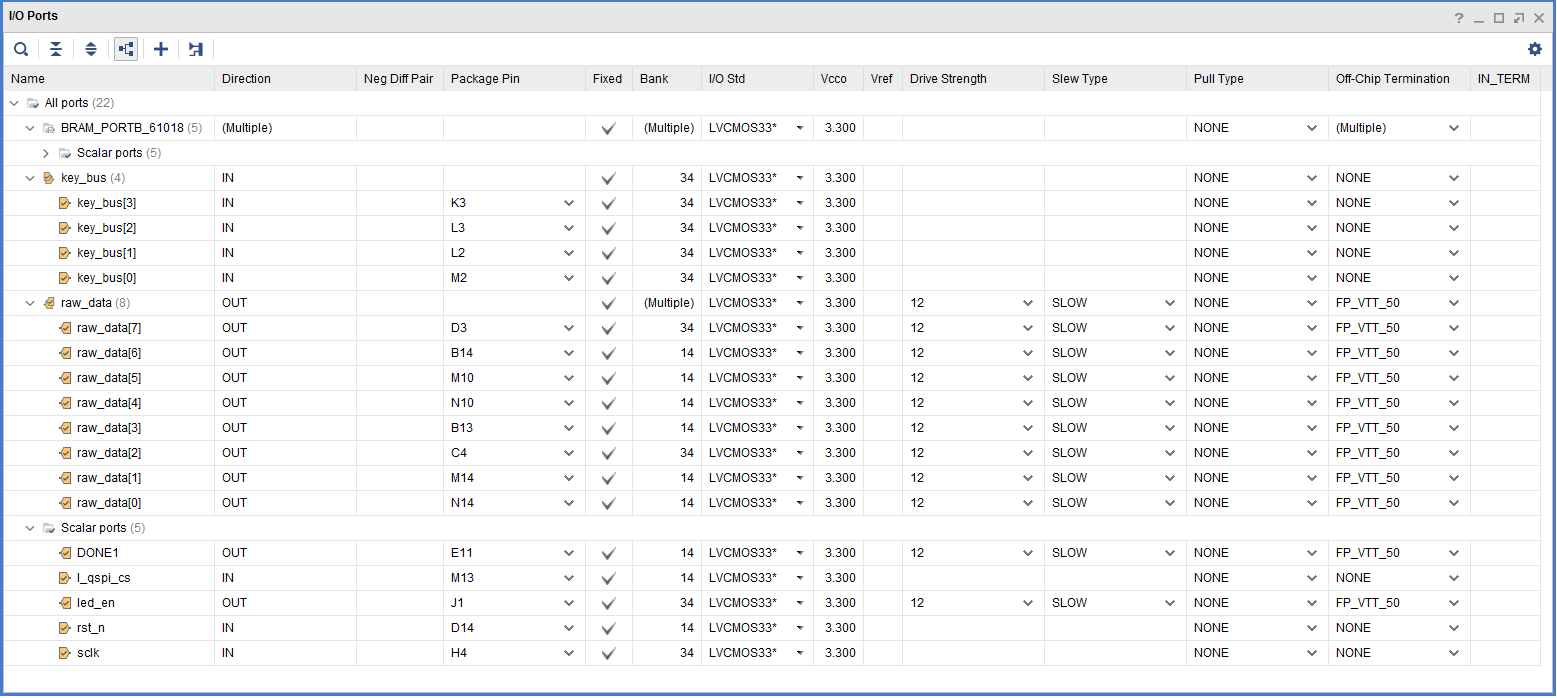
aes\_inv \_cipher\_top解密模块收到Id使能信号后，根据此时的128bit秘钥将128bit解密数据转化为128位原始扩展数据，并将数据输出到data\_ compression模块中且使能done信号；

data\_ compression模块将128bie解密后的原始扩展数据，压缩为8bit的原始数据，并将其输出到外部IO，同时拉高DONE输出使能标志信号和en控制信号；

LED\_control模块在接收到en信号后将raw\_data读入到内部men中,并判断是否大于阈值,若大于则点亮led灯,小于则熄灭,此模块主要做测试使用.

# 三、IO接口说明

## 3.1 FPGA IO Ports



## 3.2原理图接口及硬件连接关系

根据FPGA IO Ports引脚分配图标，找到对应的硬件接口Package Pin，然后查找《PCB原理图Spartan+Edge+Accelerator+Board+v1.0》这个文件，就能查看所有期间原理层链接关系，PCB板卡物理层具体位置请根据原理图器件号，查找《元件位号图\_\_top Spartan Edge Accelerator Board v1.0》和《元件位号图\_bot Spartan Edge Accelerator Board v1.0\_》文件即可找到对应的位置。

如还有问题请参考《AWS\_AES\_INVERSE.XDC》文件，[或联系本文作者shuyuz@xilinx.com](mailto:或联系本文作者shuyuz@xilinx.com)。