AWS\_aes加密使用说明书

# 程序功能

## 1.1概述

本设计主要功能是发送者将板卡ADC位置（见下图1蓝色圆圈标注位置）的输入数据进行aes算法的加密处理，加密密钥可以通过外部拨码开关随时变更。加密后的数据通过QSPI串行通信接口发送到ESP32。

后续处理是将ESP32读取的数据传输到AWS云端。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。

对应解密模块是将数据在AWS云上下载到接收者的ESP32上，在通过QSPI传输到FPGA进行解密，最后将揭解密据通过IO口输出出来。

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。

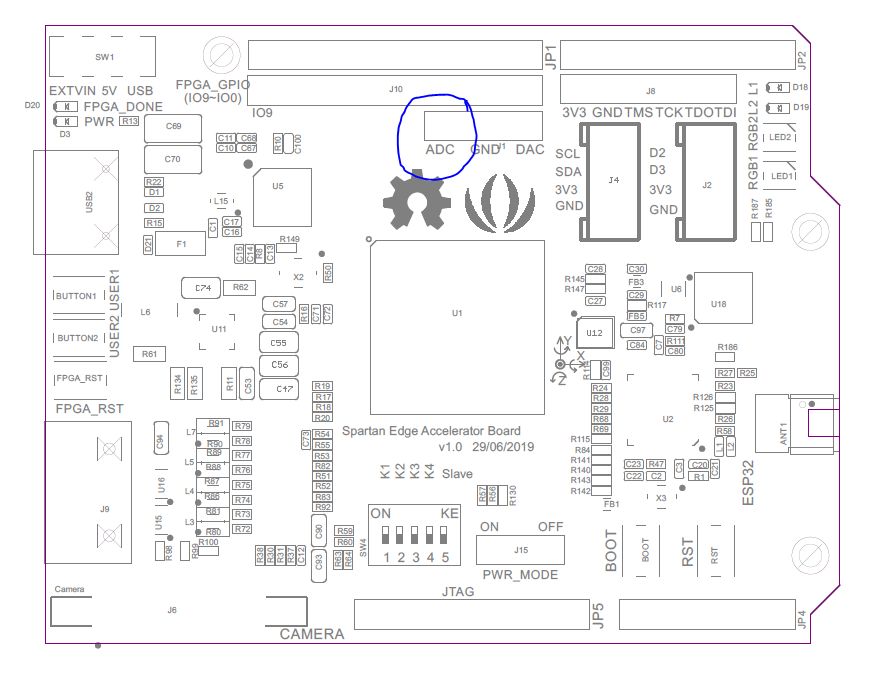


图1

## 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、加密程序架构

## 2.1 架构图

AWS\_aes

ad\_data\_in[3:0]

rst\_n

sclk

ADC\_CLK

ADC\_EN\_N

I\_qspi\_clk

I\_qspi\_cs

qspi\_data[3:0]

led\_en

key\_bus[3:0]

## 2.2 架构使用说明

AWS\_aes是一个秘钥可变动的模拟传感器AES加密算法，秘钥通过4位拨码开关加载，可随时变更,注意：密钥变更必须重新复位，点击板卡上的复位键即可；

加载秘钥后模拟数据通过ADC输出8bit数字量，数字量通过AES算法加密输出为128位的加密数据；

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；

最后算法加密后的程序可以通过QSPI通信协议传输到其他控制器上，例如测试板上的ESP32。

所以只需要通过QSPI读取RAM中对应地址的数据就可以读取到经过AES加密的128位模拟量数据。

注意: 整个模块复位后不可立即读RAM的数据，需要等秘钥加载和AD数据传输到RAM后才能读取，本设计AES采用全流水，为了保险仍需要1s中的数据加载时间。

## 2.3 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；

ad\_data\_in：8位ADC数字输入端口；

ADC\_EN\_N: ADC使能端口；

ADC\_CLK: ADC时钟输出端口；

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；

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。

## 2.4 内部架构说明

### 2.4.1 内部架构图

rst\_n

sclk

key\_

128test

4bit转128bit

key\_bus[3:0]

K1

K2

K3

K4

light\_

sensor

8bit转128bit

ADC\_CLK

ADC\_EN\_N

ad\_data

\_in[7:0]

analog

signal

light\_

sensor

ADC

aes\_cipher\_top

aes加密模块

en

ad\_128

key\_128

done

ram\_count

RAM

QSPI\_

slave

aes\_128data

Id

I\_qspi\_clk

I\_qspi\_cs

qspi\_data[3:0]

ESP

32

**AWS\_**

**aes**

led\_en

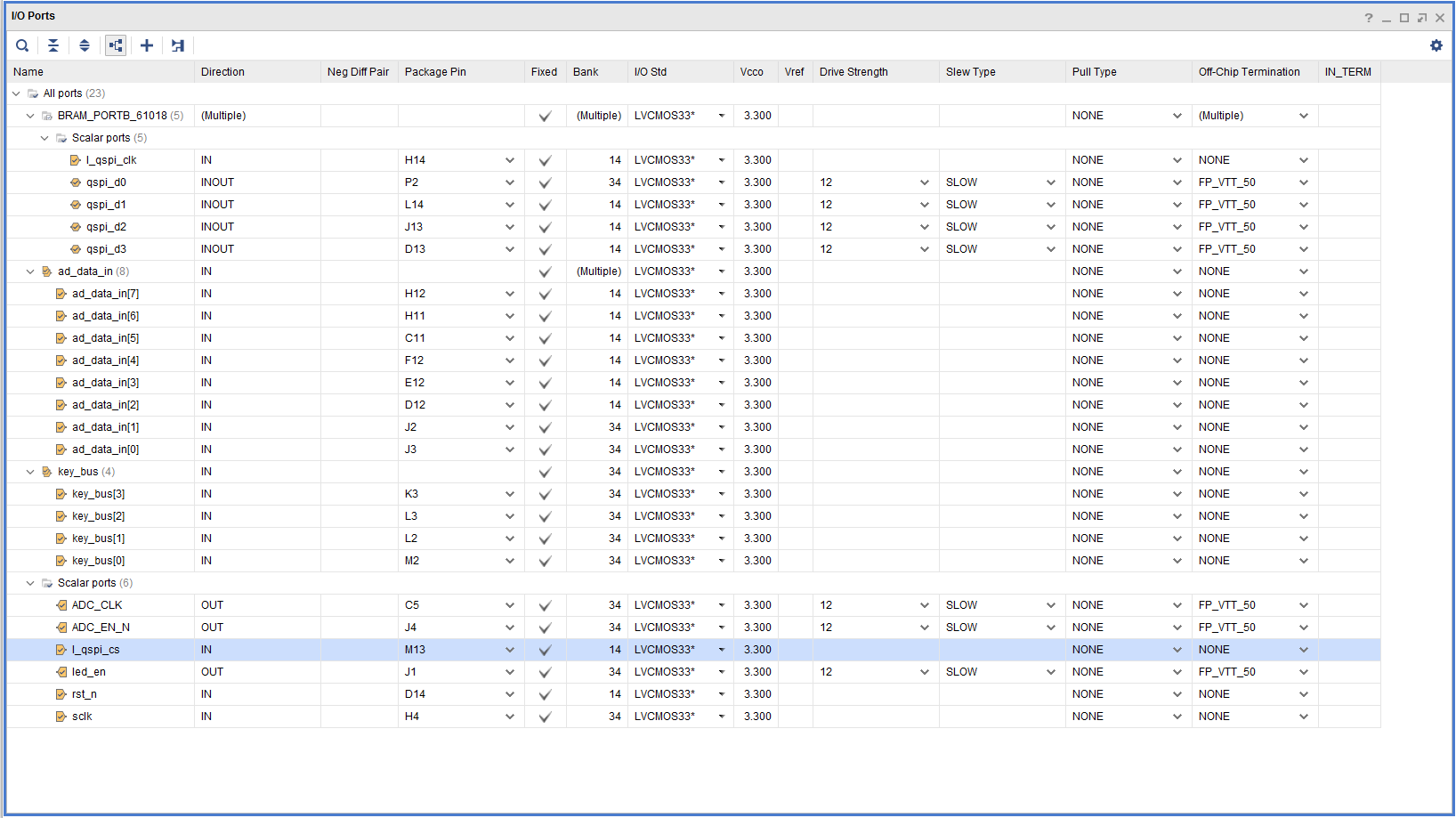
LED

### 2.4.2 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light\_sensor开始加载AD数据，并将8bit数据扩展成为128bit的AES算法数据，数据扩展完成后同时将128bit算法数据和Id使能信号输出到AES算法模块；aes\_cipher\_top算法模块收到Id使能信号后，根据此时的128bit秘钥将128bit数据转化为128位AES加密数据，并将数据存入ram\_count中；ram\_count将128bit数据拆分成每组8bit的数据，并以此存储到RAM中；存储到RAM中的起始地址为8'b0000\_0010，由于数据一共16组所以RAM的尾地址为8'b0001\_0001；最后通过QSPI\_slave模块和外部进行数据交互，交互的通信协议为QSPI。

# 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.XDC》文件，[或联系本文作者shuyuz@xilinx.com](mailto:或联系本文作者shuyuz@xilinx.com)。