**2020年新工科联盟-Xilinx暑期学校团队项目设计文档**

**设计文稿提交格式**

**(Project Paper Submission Template)**

|  |  |
| --- | --- |
| **作品名称** | MD5加密校验 |
| **板卡型号** | Spartan-7XC7S15 |
| **所在班级** | 通信工程2018-02班 |
| **成员姓名、学号、学校** | 王天淏 2018112800 西南交通大学  丁桢炎 2018112798 西南交通大学 |
| **Github链接** | <https://github.com/fuqin-feilong/MD5_CRC> |

**第一部分**

设计概述 /Design Introduction

（1.请概括地描述一下你的设计，可包括本设计目的、学习到的知识点、应用方向或者设想的应用场景等；2. 经组内成员讨论后以表格的形式描述项目中各成员在项目中发挥的作用或者贡献百分比；3.作品的展示照片）

1.设计的目的：利用FPGA提升MD5加密的运算速度

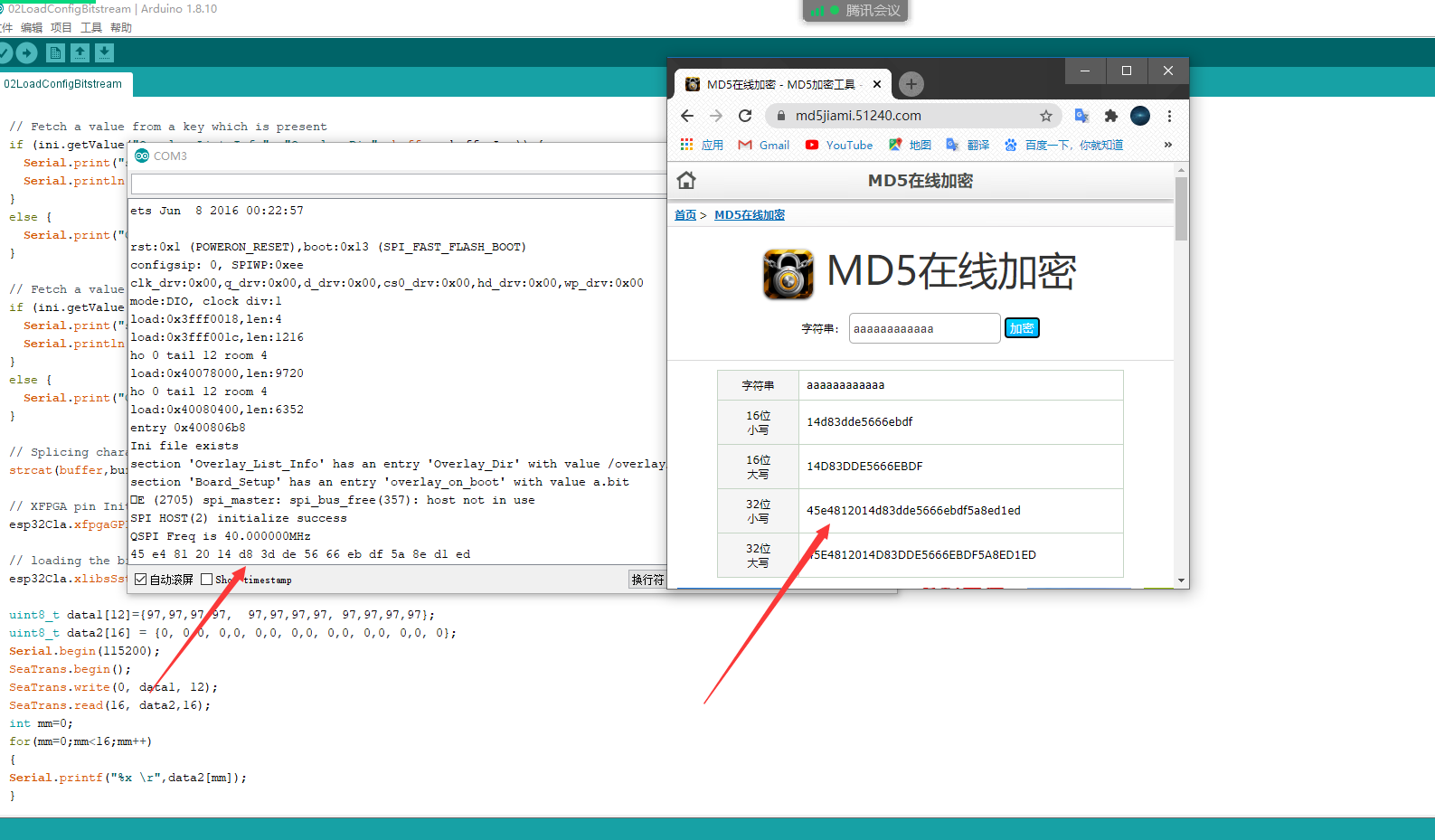
相关知识：MD5加密算法、qspi串口通信、esp32编程开发

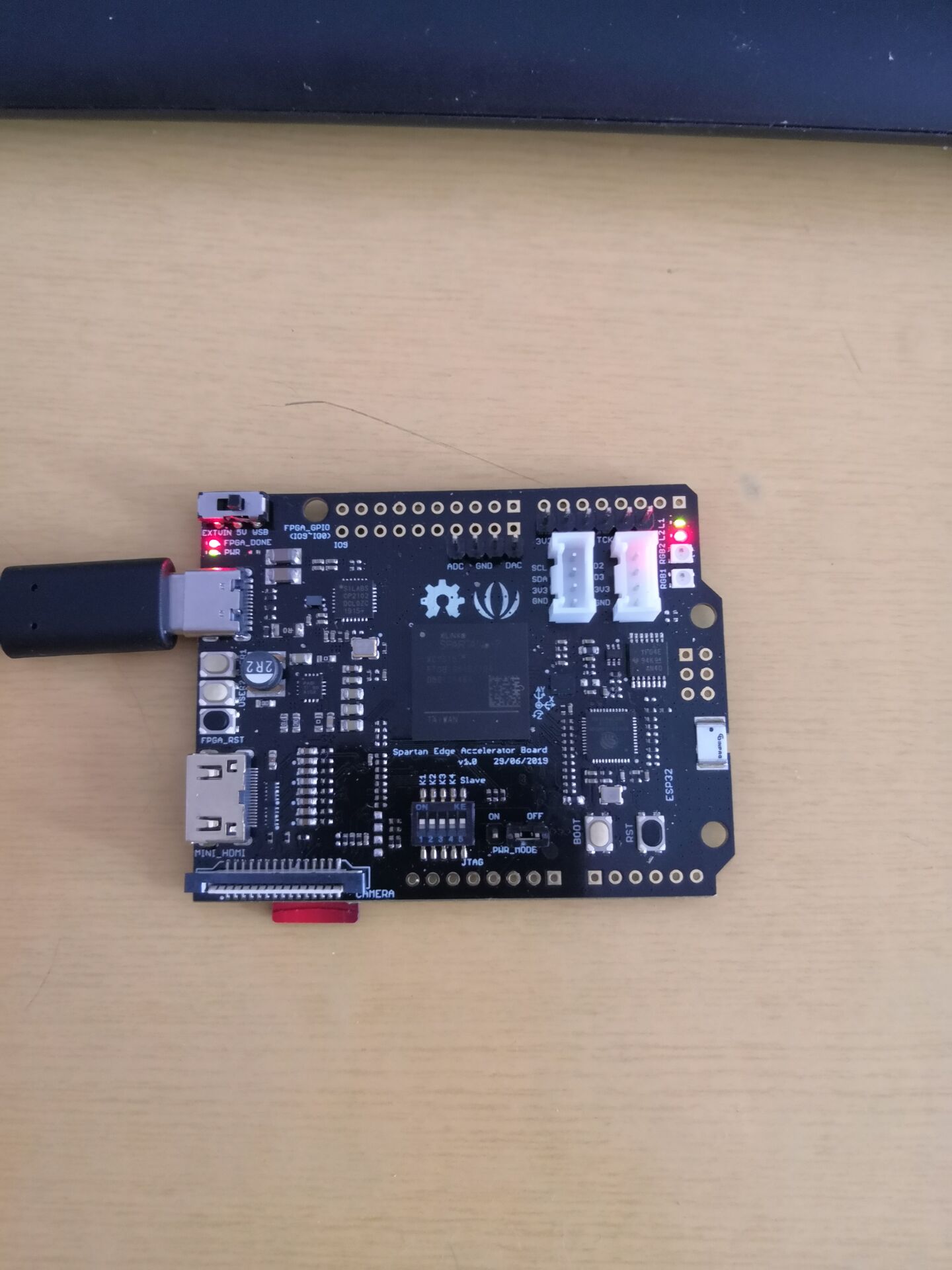
应用方向：可将FPGA与传统CPU、MCU建立通信利用FPGA并行计算加速的特性，提升传统处理器的算力。

2.成员贡献：

|  |  |
| --- | --- |
| 成员 | 负责内容 |
| 王天淏 | MD5加密算法的编写、仿真、调试。利用QSPI在FPGA建立从机通信模块，实现esp32与FPGA的数据通信，通过计算机串口控制esp32,控制FPGA的数据输入输出。实现直接从串口发送所要加密数据，并且可直接读取所得MD5加密hash值。 |
| 丁桢炎 | MD5加密算法的研究、编写、调试、仿真。加入QSPI通信后的调试、修改、仿真以及硬件的调试。 |

3.作品展示照片：





在ardunio中编写发送数据程序，发送12位“97”（字母a的ascii码），打开串口即可返回MD5加密的hash值,经验证所得MD5加密结果正确。

**第二部分**

系统组成及功能说明 /System Construction & Function Description

（请对作品的1. 计划实现及已实现的功能；2. 项目系统框图；3. 使用的技术方向做说明）

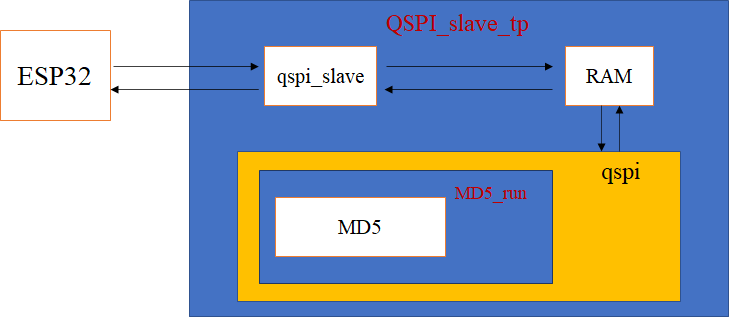
计划实现：

研究MD5加密校验算法原理，参考相关文献论文，完成其代码实现，结合暑期学校所学FPGA知识，在FPGA上运用MD5校验算法进行RTL仿真，并且结合ESP32与FPGA的QSPI通信，将接收到的信息进行MD5校验。

已实现功能：

完成了MD5校验算法的verilog代码实现，并完成了RTL仿真，结合QSPI通信，将从ESP32接收到的信息在FPGA中进行MD5校验，通过串口可以直接将加密结果返回到串口监视器，利用arduino烧写.bit文件后在开发板上运行正确。

项目系统框图：



技术方向：

本项目的核心是MD5校验算法，MD5码以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位[散列值](https://baike.baidu.com/item/%E6%95%A3%E5%88%97%E5%80%BC/10398613)。

其次扩展结合了QSPI通信，ESP32搭建QSPI传输环境后，可以作为QSPI通信主机与FPGA进行数据交互。QSPI通信模块将ESP32传输的QSPI信号解析为指令、地址、数据，将对应的数据存在FPGA侧RAM的对应地址中。

**第三部分**

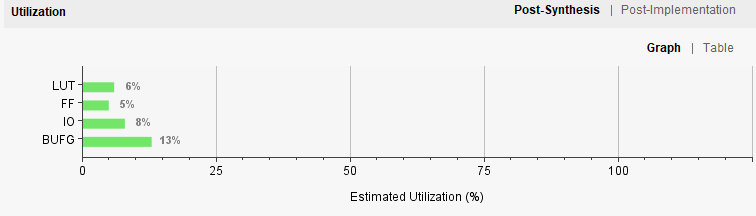
完成情况及性能参数 /Final Design & Performance Parameters

（作品已实现的功能及性能指标）

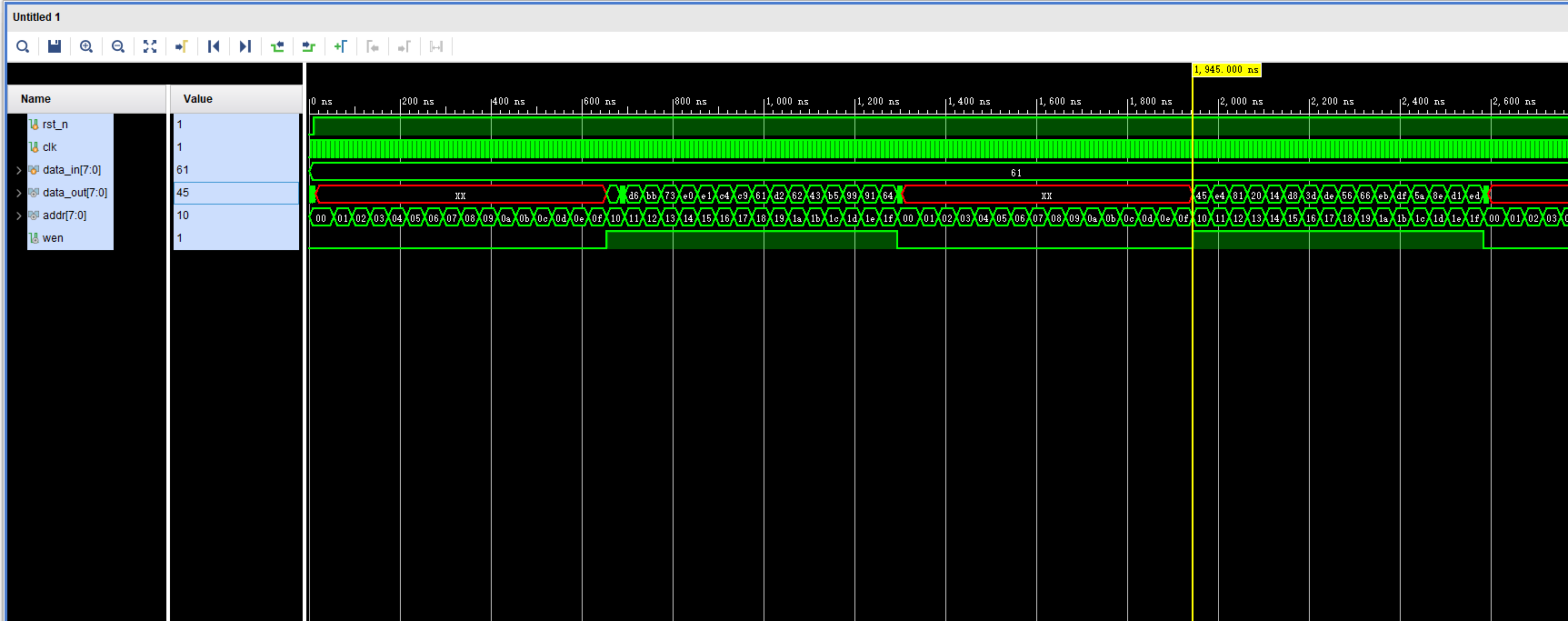
已实现的功能：利用QSPI在FPGA建立从机通信模块，实现esp32与FPGA的数据通信，通过计算机串口控制esp32,控制FPGA的数据输入输出。实现直接从串口发送所要加密数据，并且直接读取所得MD5加密hash值返回到计算机串口监视器。

性能指标：

1.占用资源：



2.仿真计算运算速度



在仿真运行到1945ns时出现正确hash值，经计算得到运算数据流65.809M/s.

**第四部分**

总结 /Conclusions

（谈一谈完成暑期学校课程后的收获与感想。请每位组员分开写。）

丁桢炎：本次暑期学校教会了我们很多关于FPGA软硬件方面的知识，使我们对FPGA硬件的特性、功能和使用场景等有了深刻的认识，使我们学会使用相应的软件如vivado和arduino，来完成软硬件的结合，并且复习了verilog语言。在不断的调试软硬件的过程中，不断询问老师以及和同学们探讨交流，深刻体会到FPGA中的痛与快乐。

王天淏：通过这次暑假学校，接触了在FPGA领域各个技术大牛，系统学习FPGA的基本知识。通过课后练习以及对课程案例的复现，让我对目前FPGA如何应用、如何开发有了清晰的认识。在完成作业的过程中会遇到很多问题，老师们也都会帮助解决问题，在自己思考问题如何解决的过程中，提升了运用FPGA的能力，也加深了对于硬件描述语言的理解。